(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年8 月31 日 (31.08.2006)

PCT

(10) 国際公開番号
WO 2006/090455 A1

(51) 国際特許分類:
G06F 12/14 (2006.01) *G06F 3/06* (2006.01)

(21) 国際出願番号: PCT/JP2005/003005

(22) 国際出願日: 2005 年2 月24 日 (24.02.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 富士通株式会社 (FUJITSU LIMITED) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 Kanagawa (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 中島 賢司 (NAKAJIMA, Kenji) [JP/JP]; 〒2118588 神奈川県川崎市中原区上小田中４丁目１番１号 富士通株式会社内 Kanagawa (JP).

(74) 代理人: 竹内 進 (TAKEUCHI, Susumu); 〒1050003 東京都港区西新橋３丁目２５番４７号 清水ビル８階 Tokyo (JP).

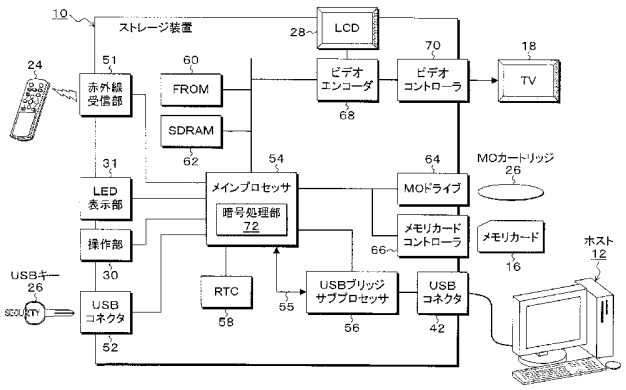
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,

/続葉有/

(54) **Title:** STORAGE DEVICE, CONTROL METHOD, AND PROGRAM

(54) **発明の名称:** 記憶装置、制御方法及びプログラム



10 STORAGE DEVICE	42 USB CONNECTOR
51 INFRARED RAY RECEPTION SECTION	66 MEMORY CARD CONTROLLER
31 LED DISPLAY SECTION	64 MO DRIVE
30 OPERATION SECTION	68 VIDEO ENCODER
26 USB KEY	70 VIDEO CONTROLLER
52 USB CONNECTOR	26 MO CARTRIDGE
54 MAIN PROCESSOR	16 MEMORY CARD
72 ENCRYPTION PROCESSING SECTION	12 HOST
56 USB BRIDGE SUB-PROCESSOR	

(57) **Abstract:** A storage device has an interface processing section performing data input into and data output from an upper-level device and processing data. A first storage medium processing section reads data from or writes data in a removable first storage medium. A second storage medium processing section reads data from or writes data in a removable second storage medium. In an encryption key input section, encryption key information is directly inputted in the storage medium without the information going through the upper-level device. In an encryption processing section, an encryption processing mode is set based on the input of the encryption key information from the encryption key input section, and the encryption processing section performs data encryption or decryption.

(57) 要約: 記憶装置は、上位装置とのデータの入出力がなされ、データを処理するインタフェース処理部を備える。第１記憶媒体処理部は着脱自在な第１記憶媒体のデータの読み出し又は書き込みを行い、第２記憶媒体処理部は着脱自在な第２記憶媒体のデータの読み出し又は書き込みを行う。暗号キー入力部は暗号キー情報が上位装置を介さず記憶装置に直接入力する。暗号処理部は暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する。

WO 2006/090455 A1

IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

記憶装置、制御方法及びプログラム

技術分野

[0001] 本発明は、パーソナルコンピュータ等のホストに対する周辺装置としての処理機能と装置単体でデータ処理や表示等を行う処理機能を備えた記憶装置、制御方法及びプログラムに関し、特に保存データを暗号化してセキュリティを確保する記憶装置、制御方法及びプログラムに関する。

背景技術

[0002] 従来、パーソナルコンピュータ等のホストの外部記憶に使用する周辺装置としての機能に加え、ホストのアプリケーションに依存せずに、例えば電子スチルカメラのメモリカードに記憶した撮影画像をMOに書き込んだり、メモリカード又はMOの画像データを装置の表示部や外部のテレビ装置に表示させるといった装置単体としての動作機能を備えた記憶装置が考えられている。

[0003] このような従来の記憶装置のセキュリティ対策としては、媒体アクセスに認証機能を持たせると同時に媒体に保存しているデータを暗号化する必要があるが、従来のセキュリティ対策は記憶装置を接続しているホストにインストールしたアプリケーションによって、記憶装置にMO(光磁気ディスク媒体)などのリムーバブル媒体を投入した際の認証とデータや画像をホストからリムーバブル媒体に書き込む際の暗号化とを行っている。

特許文献1:特開平10−083366号公報

特許文献2:特開平08−161178号公報

特許文献3:実用新案登録第3094734号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、このような従来の記憶装置にあっては、セキュリティ対策がホストに依存していたため、例えばデジタルカメラで撮影したメモリカードの画像データをMOに

コピーする場合には、記憶装置自体では暗号化ができないことから、MOに保存した後にパーソナルコンピュータに転送してアプリケーションにより暗号化し、その後に暗号化データをMOに書き込むといった煩雑な操作を必要とする。同様にMOに保存している暗号化データの復号も、暗号化データをホストに転送して復号する必要があり、手間と時間がかかって非常に使いにくい問題がある。

[0005] また記憶装置をホストから切り離して装置単体で使用する場合には、暗号化はホストのアプリケーションに依存しているために暗号化ができず、デジタルカメラで撮影したメモリカードの画像データをMOに保存しているような場合、誰でも写真画像を自由にみることができ、プライバシーを保つことができない問題がある。

[0006] 更に、このような記憶装置の利用法としては、ある記憶装置でMO等のリムーバブル媒体にデータを保存した後、他の記憶装置を使用してリムーバブル媒体からデータをコピーしたりビューワに表示する媒体を持ち回す運用ができるが、ホストに依存したセキュリティ対策では、他の記憶装置が同じ暗号化アプリケーションをもったホストに接続されていない限り、暗号化データを格納したリムーバブル媒体の持ち回りによる記憶装置の利用はできない問題がある。

[0007] 本発明は、ホストに依存することなく装置側でセキュリティ対策を簡単且つ確実に確立して利用できる記憶装置、制御方法及びプログラムを提供することを目的とする。

課題を解決するための手段

[0008] この目的を達成するため本発明は次のように構成する。

[0009] (装置)

本発明は、上位装置とのデータの入出力がなされ、データを処理するインタフェース処理部を備えた記憶装置であって、着脱自在な第1記憶媒体のデータの読み出し又は書き込みを行う第1記憶媒体処理部と、着脱自在な第2記憶媒体のデータの読み出し又は書き込みを行う第2記憶媒体処理部と、暗号キー情報が上位装置を介さず記憶装置に直接入力される暗号キー入力部と、暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する暗号処理部とを備えたことを特徴とする。

[0010] ここで、暗号処理部は、暗号処理モードを設定した際に、上位装置又は第2記憶媒体からのデータを暗号キー情報に基づいて暗号化データに変換して第1記憶媒体に記憶するか、または第1記憶媒体からの暗号化データを暗号キー情報に基づいて復号して上位装置、第2記憶媒体又は自己のディスプレイに転送する。

[0011] 暗号処理部は、暗号処理モードを設定した際に、上位装置から受信した暗号化データを暗号キー情報に基づいて更に暗号化して2重暗号化データに変換して第1記憶媒体に記憶し、第1記憶媒体から上位装置に転送する2重暗号化データを暗号キー情報に基づいて暗号化データに復号する。

[0012] 暗号キー入力部はUSBポートを備えたUSBインタフェースであり、USBポートに接続したUSBキー(USBデバイス)に記憶された暗号キー情報を読み出して暗号処理部に入力する。

[0013] 暗号キー入力部は赤外線受信部であり、リモートコントローラから赤外線により送信された暗号キー情報を受信して暗号処理部に入力する。

[0014] 暗号キー入力部はユーザ操作部であり、操作入力された暗号キー情報を暗号処理部に転送する。

[0015] 暗号キー入力部は、暗号キー情報としてパスワードと暗号キーを入力し、暗号処理部は、暗号キーにより予め保存された暗号パスワードを復元して入力パスワードと比較し、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定する。

[0016] 暗号キー入力部は、暗号キー情報としてパスワードを入力し、暗号処理部は、パスワードから暗号キーを生成して予め保存された暗号パスワードを復元して入力パスワードと比較し、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定する。

[0017] 暗号処理部は、暗号キー情報が存在しない場合は、第1記憶媒体又は第2記憶媒体からの暗号化データの読出要求に対し表示処理部により暗号キー情報の入力を要求するエラーメッセージを表示させる。

[0018] 暗号処理部は、暗号キー情報が存在しない場合は、第1記憶媒体又は第2記憶媒体からの暗号化データの読出要求に対し読み出しを禁止して暗号化データの存在を隠蔽する。

[0019] 暗号処理部は、暗号キー情報が存在しない場合は、第1記憶媒体又は第2記憶媒体に格納したファイルメニューに非暗号化データのみを表示し、暗号化データの存在を隠蔽する。

[0020] (方法)

本発明は、記憶装置の制御方法を提供する。即ち本発明は、上位装置とのデータの入出力がなされ、データを処理するインタフェース処理部を備えた記憶装置の制御方法に於いて、

着脱自在な第1記憶媒体のデータの読み出し又は書き込みを行う第1記憶媒体処理ステップと、

着脱自在な第2記憶媒体のデータの読み出し又は書き込みを行う第2記憶媒体処理ステップと、

暗号キー情報が上位装置を介さずに記憶装置に直接入力される暗号キー入力ステップと、

暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する暗号処理ステップと、

を備えたことを特徴とする。

[0021] (プログラム)

本発明は,記憶装置のコンピュータで実行されるプログラムを提供する。即ち、本発明のプログラムは、上位装置とのデータの入出力がなされ、データを処理するインタフェース処理部を備えた記憶装置のコンピュータに、

着脱自在な第1記憶媒体のデータの読み出し又は書き込みを行う第1記憶媒体処理ステップと、

着脱自在な第2記憶媒体のデータの読み出し又は書き込みを行う第2記憶媒体処理ステップと、

暗号キー情報が上位装置を介さずに記憶装置に直接入力される暗号キー入力ステップと、

暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する暗号処理ステップと、

を実行させることを特徴とする。

[0022] なお、本発明の制御方法及びプログラムの詳細は、記憶装置の場合と基本的に同じになる。

発明の効果

[0023] 本発明によれば、記憶装置に暗号情報キーとして機能するメモリステックなどのUSBキーを挿入接続することで、暗号キー情報が自動的に入力されて暗号認証処理が行われ、認証成功で暗号処理モードが設定され、ホストやカード媒体(第2記憶媒体)からディスク媒体(第1記憶媒体)に保存するデータの暗号化とディスク媒体から読み出した暗号化データの復号を、上位装置に依存せずに装置自体で処理することができ、リムーバブルなディスク媒体やカード媒体に保存して利用するデータのセキュリティ対策を簡単且つ確実にとることができる。

[0024] またホストと接続せずに装置単体として動作させる際のカード媒体とディスク媒体との間のコピー処理やディスプレイに表示する際にも、暗号キー情報を格納した例えばUSBキーを挿入するだけで、通常データの暗号化によるコピー、暗号化データの復号コピー、暗号化データの復号表示が簡単できる。

[0025] また暗号処理を解除したい場合には、暗号キー情報を格納した例えばUSBキーを取り外すだけで通常モードとすることができる。

[0026] 更に、暗号化データを保存したリムーバブルなディスク媒体やカード媒体を他の装置で利用する持ち回り運用は、媒体と一緒に暗号キー情報を格納したUSBキーを持参すればよく、装置が変わっても暗号処理をそのまま利用することができる。

[0027] 更に、暗号キー情報の入力は、USBキー以外に、記憶装置の操作に使用するリモートコントローラや記憶装置に設けている操作釦によっても入力することができ、このためUSBキーを忘れたような場合でも、例えばパスワードを釦操作で入力することにより、暗号認証処理を有効として暗号処理モードでの運用ができる。

図面の簡単な説明

[0028] [図1]本発明の記憶装置とその利用形態の説明図

[図2]本発明の記憶装置の平面及び正面図

[図3]本発明の記憶装置の左右の側面図

[図4]本発明による記憶装置の機能構成の実施形態を示したブロック図

[図5]USBキー使用して、MO媒体を暗号化媒体とした場合の本発明による制御処理のフローチャート

[図6]図5に続く制御処理のフローチャート

[図7]図6に続く制御処理のフローチャート

[図8]USBキーからパスワードと暗号キーを入力する認証処理のフローチャート

[図9]USBキーからパスワードと暗号キーを入力する他の認証処理のフローチャート

[図10]USBキーからパスワードのみを入力する認証処理のフローチャート

[図11]USBキーとしてパスワードのみを入力する他の認証処理のフローチャート

[図12]USBキーを使用してMO媒体及びメモリカードの両方に暗号化データを格納する場合の本発明による制御処理のフローチャート

[図13]図12に続く制御処理のフローチャート

[図14]図13に続く制御処理のフローチャート

[図15]リモートコントローラにより暗号キー情報を入力する場合の制御処理のフローチャート

[図16]装置操作部により暗号キー情報を入力する場合の制御処理のフローチャート

発明を実施するための最良の形態

[0029] 図1は本発明による記憶装置とその利用形態の説明図である。図1において、本発明の記憶装置10は、上位装置となるパーソナルコンピュータなどのホスト12に接続されて外部記憶などの周辺装置として使用することができる。また本発明の記憶装置10は、ホスト12に対する接続を切り離した単体装置として使用することもできる。

[0030] また、例えば、デジタルカメラやビデオレコーダなどのデジタル家庭用電化製品のコントローラ(組み込みコンピュータ)を上位装置とし、インタフェース接続して、それらのデータ転送や保存等を目的とした記憶装置として使用することが可能である。

[0031] 記憶装置10は、第1記憶媒体となるMOカートリッジ14の処理機能と、電子スチルカメラや携帯電話端末などの画像データを格納した第2記憶媒体となるメモリカード1

6−1，16−2の処理機能を備えており、後の説明で明らかにするように、装置自体に液晶ディスプレイを持つと共に、外部にテレビ装置18、オーディオシステム20−1あるいはヘッドホン20−2を接続することができる。

[0032] なお、本実施形態ではMOカートリッジの処理機能を備えたもので記憶装置を説明するが、DVDやCD等の可搬型記憶媒体を処理する処理機能に置き換える記憶装置であっても良い。

[0033] カード状媒体の処理機能は、サイズに応じて、メモリステック、メモリカード、スマートメディア、マイクロドライブ、コンパクトフラッシュ(R)、ピクチャカード(変換アダプター対応)などに対応可能になっている。

[0034] 更に、記憶装置10に対しては暗号キー情報を格納したUSBキー26を必要に応じて接続することができ、USBキー26を接続した状態で記憶装置10は暗号処理モードで動作し、一方、USBキー26を接続しなければ通常モード(非暗号処理モード)で動作する。

[0035] 記憶装置10をホスト12に接続した状態で周辺装置として使用する場合には、MOカートリッジ14やメモリカード16−1，16−2に対するホスト12からのコマンドによる書込みまたは読出しが実行できる。この場合、USBキー26の接続により暗号処理モードとなっている場合には、ホスト12から例えばMOカートリッジ14に対する書込データを暗号化して書き込み、MOカートリッジ14に格納している暗号化されたデータは復号してホスト12に転送することになる。

[0036] 一方、装置単体動作としては、装置自身に設けている操作部の釦操作により、MOカートリッジ14とメモリカード16−1，16−2間のデータの移し替え(コピー)、MOカートリッジ14またはメモリカード16−1，16−2に記憶している画像データの読出しによる装置に設けている液晶ディスプレイまたは外部のテレビ装置18に対する画像表示ができる。

[0037] 装置単体動作の場合にも、USBキー26が挿入接続されている場合には暗号処理モードが設定され、例えばメモリカード16−1，16−2のオリジナルデータをMOカートリッジ14に移し替えるコピー処理の際に暗号化が行われる。また、MOカートリッジ14に格納された暗号化データを読み出してテレビ装置18で再生する場合には、読み

出した暗号化データを復号して表示させることになる。

[0038] 図2は本発明による記憶装置10の平面及び正面図である。図2(A)の平面図から明らかなように、記憶装置10の上部中央には液晶ディスプレイ28が設けられ、その下側に操作部30と表示用のLED36を設けている。操作部30には、決定ボタン32、方向キー34−1ー34−4及びキャンセルボタン34−5が設けられている。操作部30の方向キー34−1ー34−4、決定ボタン32及びキャンセルボタン34−5を使用することで、液晶ディスプレイ28に表示された初期画面のメニュー選択により装置単体動作を行わせることができる。

[0039] 図2(B)の正面図を見ると、そこにはコンパクトフラッシュ(R)カード用のメモリカードスロット38−1と、SDカードメモリスティック・スマートメディア用スロットとして用いるメモリカードスロット26−2、及びリモコン受光部50が設けられている。

[0040] 図3は本発明による記憶装置10の左右の側面図であり、図3(A)の左側面には電源スイッチ40、ホスト接続用のUSBコネクタ42、テレビコネクタ44及び電源コネクタ(DCジャック)46が設けられ、右側面にはMOスロット48、リモコン受光部50、更にUSBキーを接続するUSBコネクタ52を設けている。

[0041] 図4は本発明による記憶装置10の回路構成の実施形態を示したブロック図である。図4において、本発明の記憶装置10の回路部には、ホスト12の入出力処理を実行するサブプロセッサとして、この実施形態にあってはUSBブリッジサブプロセッサ56を設けている。USBブリッジサブプロセッサ56は、具体的にはUSBブリッジ用のLSIで実現される。なお、ホスト12を接続するインタフェースとして、この例ではUSBブリッジサブプロセッサ56を例にとっているが、これ以外にIEEE1394などのホストインタフェースブリッジ用LSIをサブプロセッサとして設けるようにしてもよい。

[0042] USBブリッジサブプロセッサ56に加え、記憶装置10には更に、装置単体動作におけるデータ転送と画像表示処理を実行するメインプロセッサ54を設けている。メインプロセッサ54はUSBブリッジサブプロセッサ56を含む装置全体の管理を行い、各デバイスの処理状況、動作状況を監視し、ホスト12との間の入出力制御及び装置単体処理を必要に応じて選択的に実行させる。

[0043] 更に、メインプロセッサ54には暗号処理部72が設けられる。暗号処理部72は、US

Bコネクタ42にUSBキー26を接続した場合に、USBキー26に保存している暗号キー情報を読み込み、必要に応じて認証処理を行った後に暗号処理モードを設定し、ホスト12に接続された周辺装置として動作する際には、ホスト12からのオリジナルデータを暗号化してMOカートリッジ14に書き込み、またMOカートリッジ14から読み出した暗号化データを復号してホスト12に転送する。また暗号化処理部72は、ホスト12との接続を切り離した単体動作の場合には、メモリカード16のオリジナルデータを暗号化してMOカートリッジ14に書き込み、MOカートリッジ14の暗号化データを読み出し、復号した後に、液晶ディスプレイ28やテレビ装置18に表示する。

[0044] 記憶装置10の記憶デバイスとしては、MOドライブ64とメモリカードコントローラ66が設けられる。MOドライブ64に対しては、MOカートリッジ14を装着して、書込み、読出しができる。メモリカードコントローラ66に対しては、そのスロットに挿入したメモリカードに対するデータの書込みと読出しができる。

[0045] MOドライブ64及びメモリカードコントローラ66は、メインプロセッサ54のバスに接続されている。ここで、メインプロセッサ54とUSBブリッジサブプロセッサ56のバスはUSBバスであるが、メインプロセッサ54とMOドライブ64及びメモリカードコントローラ66のバスは例えばATAバスとなり、メインプロセッサ54の暗号化処理部72で暗号化されたデータは、MOドライブ64及びメモリカードコントローラ66との間のATAバス上では暗号化データとして送受信されることになる。

[0046] メインプロセッサ54のバスには、更にFROM60及びSDRAM62が設けられる。FROM60には、メインプロセッサ54が実行するプログラムや暗号認証に必要な情報が予め記憶されている。

[0047] SDRAM62は、メインプロセッサ54の暗号処理部72により、例えばホスト12からのオリジナルデータをMOカートリッジ14に格納する際の暗号化処理のメモリ領域として使用される。また、装置単体動作の際にメモリカード16のオリジナルデータを暗号化してMOカートリッジ14に格納する際のメモリ領域としてもSDRAM62が使用される。

[0048] メインプロセッサ54に対しては、操作部30、LED表示部31、USBキー26を接続するUSBコネクタ52、更にリアルタイムクロック(RTC)58が接続されている。なお記

憶装置10には図示しない電源供給ユニットが設けられ、外部のACアダプタによる電源供給を受けて、例えばDC5ボルト、DC3．3ボルト及びDC2．5ボルトの、各回路部に必要な電源を供給している。

[0049] 更に、メインプロセッサ54に対してはビデオエンコーダ68が設けられ、ビデオエンコーダ68の出力は装置自身に設けた液晶ディスプレイ28に接続されると同時に、外部のテレビ装置18を接続するためのビデオコントローラ70に接続される。

[0050] メインプロセッサ54とUSBブリッジサブプロセッサ56の間は制御ライン55により接続されており、両者間で処理要求とその応答を行うことができる。またメインプロセッサ54は、ホスト12のUSBコネクタ42に対する接続を判別する際に、ホスト12によるUSBブリッジサブプロセッサ56に対する入出力処理を実行可能とする周辺機動作モードを設定し、この状態で操作部30のスイッチ動作で装置単体動作の処理要求を判別した場合には、USBブリッジサブプロセッサ56によるホスト12との入出力処理を解除して装置を単体動作モードに設定する。なお電源投入時にホスト12のUSBコネクタ42に対する接続が検出されなかった場合には、単体動作モードの設定で立ち上がることになる。

[0051] メインプロセッサ54に設けた暗号処理部72は、記憶装置10の電源投入による立上げ時に、USBコネクタ52に対するUSBキー26の接続の有無をチェックし、USBキー26の接続があれば暗号処理モードを設定して動作し、USBキー26が接続されていない場合には通常モードを設定して動作することになる。もちろん、通常モードを設定した動作状態でUSBコネクタ52に対するUSBキーの接続を検出すると、その段階で暗号処理モードを設定して動作することになる。即ち、本発明の記憶装置10にあっては、USBキー26を接続すれば暗号処理が行われ、USBキー26を外せば通常処理が行われることになる。

[0052] 暗号処理部72によるオリジナルデータの暗号化は、USBキーに記憶されている暗号キー情報キーに基づいた暗号化処理を実行してオリジナルデータを暗号化データに変換するエンコード機能と、暗号化データを元のオリジナルデータに変換するデコード機能を備えている。

[0053] 暗号処理部72で使用する暗号化アルゴリズムとしては、1つの鍵で暗号化し同じ鍵

で復号化する共通鍵暗号アルゴリズム、あるいは公開鍵で暗号化し秘密鍵で復号化する公開鍵暗号方式など、適宜の暗号化アルゴリズムを使用することができる。共通鍵暗号方式としては、DES(DATA Encryption Standard)や、AES(Advanced Encryption Standard)などが使用できる。また共通鍵暗号方式としてはRASなどが使用できる。

[0054] 暗号処理部72による暗号化処理は、ホスト12に接続した場合の周辺機動作モードと、ホスト12との接続を切り離した単体動作モードで異なる。

[0055] 周辺機動作モードにあっては次の暗号処理を行う。

・ ホスト12からのライトコマンドによるライトデータを暗号化してMOカートリッジ14に書き込む。

・ ホスト12からのリードコマンドに対し、MOカートリッジの暗号化データを復号して転送する。

[0056] なお、ホスト12からメモリカードコントローラ66に挿入されたメモリカード16に対しても、MOカートリッジ14の場合と同様に、ライトで暗号化、リードで復号の処理を行うことができる。

[0057] 一方、装置単体動作モードにあっては、異なる媒体間のコピー処理と媒体から液晶ディスプレイ28に表示する表示処理とがある。装置単体動作モードにおけるコピー処理は次の暗号化処理を行う。

・ メモリカード16のオリジナルデータを暗号化してMOカートリッジ14にコピーする。

・ MOカートリッジ14の暗号化データを復号化してメモリカード16にコピーする。

・ MOカートリッジ14の暗号化データをそのままメモリカード16にコピーする。

[0058] また装置単体動作モードにおける表示処理の際には、次の暗号処理を行う。

・ MOカートリッジ14の暗号化データを復号して、液晶ディスプレイ28またはテレビ装置18に表示する。

・ メモリカード16の暗号化データを復号して、液晶ディスプレイ28またはテレビ装置18に表示する。

[0059] 更に本発明の暗号化処理部72にあっては、基本的にはUSBキー26が接続されていれば暗号処理モードを設定し、接続していなければ通常モードを設定するが、更

にUSBキー26にパスワードなどの認証情報を記憶しておき、パスワードと暗号キーに基づいて暗号認証を行い、認証に成功した場合に暗号処理モードを設定し、認証失敗で通常モードを設定することもできる。この認証処理を暗号処理モードの設定に組み合わせることで、記憶装置10におけるセキュリティを更に高めることができる。

[0060] また本発明の記憶装置10にあっては、USBキー26により暗号処理を行う際に、暗号処理を行う媒体を特定するため、例えばMOカートリッジ14に対し初期設定により暗号化媒体とするか否かの設定(媒体フォーマット時／初期化時に所定の暗号キーによる暗号化媒体として予め設定)を行って、暗号化媒体を示す情報を媒体システム領域などに保存しておき、暗号化媒体であることを認識して、暗号キーに基づく認証処理の下に暗号処理モードを設定することができる

更に本発明の記憶装置10は、USBキー26による暗号処理モードの設定以外に、リモートコントローラ24による暗号キー情報の入力、または操作部30のボタン操作による暗号キー情報の入力によっても、暗号処理モードを設定することができるようにしている。

[0061] 図5はUSBキーにより暗号動作モードを設定し、且つMO媒体に暗号化データを格納する場合の本発明による制御処理のフローチャートである。

[0062] 図5において、記憶装置10の電源を投入すると、まずステップS1でUSBキー26のUSBコネクタ52に対する接続の有無をチェックし、USBキー26があればステップS2に進み、ストレージ媒体の内容を確認する。このストレージ媒体の内容は、そのとき記憶装置10にセットされている媒体であり、例えばMOカートリッジ14やメモリカード16の内容を確認する。

[0063] 次にステップS3でストレージ媒体が暗号化媒体か否かチェックする。この処理にあっては、暗号化媒体としてMOカートリッジ14が設定されていることから、MOカートリッジ14が投入されていれば暗号化媒体ありと判定する。

[0064] 次に、ステップS4でUSBキー26を用いた暗号キーに基づく認証処理を実行する。この暗号キーに基づく認証処理については、後の説明で明らかにする。ステップS5で認証成功を判別すると、ステップS6に進み、暗号処理モードを設定する。認証失敗であれば、ステップS20で通常モードを設定する。

[0065] ステップS6で暗号処理モードを設定した場合には、ステップS7で上位装置としてのホスト12の接続の有無をチェックし、接続があればステップS8に進み、周辺機器動作モードを設定する。接続がなければ、ステップS14で単体動作モードを設定する。

[0066] ステップS8で周辺機器動作モードを設定した場合には、ホスト12からの周辺機器選択コマンドに対しMOカートリッジ14のファイル内容を転送して、ホスト画面上にファイル内容のメニューを展開し、ホスト12において記憶装置10に対するファイル選択による書込みまたは読出しができるようにする。

[0067] 続いてステップS9でホスト12からのリードコマンドの有無をチェックしており、リードコマンドを受信するとステップS10に進み、MOカートリッジ14から読み出した暗号化データを復号してホストに転送する。またステップS11でホストからのライトコマンドを受信した場合には、ステップS12でホストからのデータを暗号化してMOカートリッジ14に書き込む。このような周辺機器動作モードの処理を、ステップS13で停止指示があるまで繰り返す。

[0068] なおステップS9ーS13の周辺機動作モードの設定によるリードライト処理にあっては、停止指示があるまで周辺機器動作モードの設定状態を維持しているが、操作部30の釦操作により単体動作モードへの切替指示があった場合には、周辺機器動作モードを解除して単体動作モードに切り替えることができる。

[0069] ステップS14の単体動作モードの設定が行われた場合には、ステップS15でコピー要求の有無をチェックしており、コピー要求があると、ステップS16に進み、次の処理を行う。

・ コピー元のメニュー表示

・ コピー元がメモリカードの場合、メモリカードのデータを暗号化してMOカートリッジにコピー

・ コピー元がMOカートリッジ14の場合、暗号化データを復号してメモリカードにコピー

[0070] 続いてステップS17で表示要求の有無をチェックしており、表示要求があるとステップS18において次の処理を行う。

・ 媒体内容のメニュー表示

・ MOカートリッジの場合は暗号化データを復号して表示

・ メモリカードの場合はデータをそのまま表示

[0071] この単体動作モードにあっては、ステップS15ーS18の処理を、ステップS19で停止指示があるまで繰り返す。もちろん単体動作モード中にあっても、操作部30の釦操作で周辺機動作モードが設定された場合には、単体動作モードから周辺機動作モードに切り替えることができる。

[0072] 次に、図6のステップS20で通常動作モードが設定された場合の処理を説明する。通常動作モードがステップS20で設定されるとステップS21に進み、上位装置としてのホスト12の接続の有無をチェックする。ホストの接続があれば、ステップS22で周辺機器動作モードを設定する。

[0073] 続いてステップS23でリードコマンドの有無を判別し、リードコマンドを受信すると、ステップS24でMOカートリッジ14のデータが暗号化データか否かチェックする。暗号化データであった場合にはステップS25に進み、アクセス許可の装置設定があるか否かチェックする。

[0074] アクセス許可の装置設定の有無は、記憶装置10を最初に使用する際の初期設定で必要に応じて適宜に行われている。アクセス許可の装置設定が判別されると、ステップS26に進み、MOカートリッジ14から読み出した暗号化データをそのままホストに転送する。

[0075] 一方、ステップS25でアクセス許可の装置設定がなかった場合には、ステップS28でリードコマンドに対するアクセスを禁止し、これによってMOカートリッジ14に記憶している暗号化データをホスト12に送ることを禁止してデータを隠蔽する。

[0076] 一方、ステップS24で暗号化データでなかった場合には、ステップS27で通常のリードコマンドの場合と同様、MOカートリッジ14のデータを読み出してホスト12に転送する。

[0077] ステップS23でリードコマンドでなかった場合には、ステップS30でライトコマンドか否かチェックし、ライトコマンドであれば、ステップS31でホストからのデータをMOカートリッジ14に書き込む。ステップS23からの処理は、ステップS29で停止指示があ

るまで繰り返される。

[0078] 図6のステップS21で通常モード設定後に上位装置の接続がなかった場合には、図7のステップS32に進み、単体動作モードを設定する。単体動作モードを設定した場合には、ステップS33でコピー要求の有無をチェックし、コピー要求があれば、ステップS34でメモリカード16とMOカートリッジ14の間でコピー元からコピー先への転送コピーを行う。

[0079] この場合、メモリカード16及びMOカートリッジ14のデータをそのまま転送コピーすることになる。例えば、メモリカード16がオリジナルデータであれば、このオリジナルデータをそのままMOカートリッジ14に転送コピーする。また、MOカートリッジ14のデータが暗号化データであれば、暗号化データをそのままメモリカード16に転送コピーする。

[0080] 続いてステップS35でデータ表示要求の有無をチェックしており、データ表示要求があると、ステップS36で要求された媒体のデータが暗号化データか否かチェックする。暗号化データであれば、ステップS37でアクセス許可の装置設定の有無をチェックし、装置設定があれば、ステップS38で暗号化データであることのメッセージ表示を液晶ディスプレイ28に行った後、ステップS39で暗号キー情報の入力を要求するエラーメッセージを表示する。具体的には、USBキー26の接続を要求するエラーメッセージを表示する。

[0081] この暗号認証を要求するエラーメッセージの表示に対し、ステップS40でUSBキー26の接続を判別すると、図5のステップS2に戻り、電源投入時にUSBキー26を接続した場合と同様な処理により暗号処理モードに入ることができる。USBキー26の接続がステップS40でなければ、ステップS41で停止指示を待って処理を終了する。

[0082] 一方、ステップS36でデータ表示要求の対象となった媒体格納データが通常データであった場合には、ステップS42でMOカートリッジ14またはメモリカード16のデータを読み出して表示する。

[0083] またステップS36で暗号化データであった場合にステップS37でアクセス許可の装置要求の設定がなかった場合には、ステップS43に進み、アクセスを禁止して暗号化データの表示は行わず、これによって暗号化データの存在自体を隠蔽する。この場

合にも、ステップS44で停止指示があるまで、ステップS33からの処理を繰り返すことになる。

[0084] 図8は図5のステップS4で行われる暗号キー情報に基づく認証処理の詳細を示した説明図である。

[0085] 図8(A)は認証処理に使用する各種の情報の格納状態を示している。図8(A)において、USBキー26には、この実施形態にあってはパスワード74と暗号キー76を格納している。また暗号化媒体として使用するMO媒体15には暗号化パスワード78をユーザ領域以外の例えばシステム領域に格納している。

[0086] MO媒体15に対する暗号化パスワード78の格納は、MO媒体15を暗号化媒体として使用する際の初期設定の際にUSBキー26を使用し、USBキー26から入力したパスワード74を暗号処理部72により暗号キー76を用いて暗号化して格納している。

[0087] このようなUSBキー26及びMO媒体15を記憶装置10にセットした場合の認証処理は、図8(B)のフローチャートのようになる。この認証処理にあっては、ステップS1でUSBキー26からパスワード74と暗号キー76を読み込み、ステップS2でMO媒体15から暗号化パスワード78を読み込む。

[0088] 続いてステップS3で暗号キー76によりMO媒体15から読み込んだ暗号化パスワードを復号し、ステップS4で復号したパスワードとし、USBキー26から入力した入力パスワードを比較照合する。そして図5のステップS5のメインルーチンに戻り、ステップS5の認証成功であればステップS6で暗号処理モードを設定し、認証失敗であればステップS20で通常モードを設定する。

[0089] 図8のようなUSBキー26とMO媒体15による認証処理にあっては、USBキー26とMO媒体15の組み合わせにより、複数の本発明の記憶装置10を対象にデータを持ち周りして利用する運用が実現できる。

[0090] 図9はUSBキーからパスワードと暗号キーを入力する他の認証処理の説明図である。

[0091] 図9(A)は認証処理に必要な情報の格納状態であり、この実施形態にあってはUSBキー26にパスワード74と暗号キー76が保存され、暗号化パスワード78はMO媒体15ではなく記憶装置10の暗号処理部72、具体的には図4のSDRM62に格納され

ている。

[0092] 図9(B)は図9(A)の認証に必要な情報の格納状態における認証処理のフローチャートである。この認証処理にあっては、ステップS1でUSBキー26からパスワード74と暗号キー76を読み込み、ステップS2で暗号キーにより記憶装置10に保存している暗号化パスワード78を復号し、ステップS3で復号化したパスワードとUSBキー26から入力した入力パスワードを比較照合し、図5のメインルーチンにリターンし、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定することになる。

[0093] この図9の実施形態のように、暗号キーにより復号して認証に使用する暗号化パスワード78をMO媒体15ではなく記憶装置10そのものに保存しておくことで、USBキー26を記憶装置固有の暗号キーとして使用することができる。

[0094] 図10はUSBキーからパスワードを入力する他の認証処理のフローチャートである。図10(A)は認証処理に必要な情報の格納状態であり、この実施形態にあってはUSBキー26にはパスワード74のみが記録されており、暗号キーは記録されていない。

[0095] またMO媒体15には初期設定の際に暗号化パスワード78が保存されている。記憶装置10に設けている暗号処理部72はUSBキー26の接続で入力したパスワード74から暗号キー80を生成する暗号キー生成機能を備えている。

[0096] 図10(B)は図10(A)を対象とした認証処理のフローチャートである。この認証処理は、ステップS1でUSBキー26からパスワード74を読み込み、ステップS2で入力パスワード74から暗号キー80を生成する。

[0097] 続いてステップS3でMO媒体15から暗号化パスワード78を読み込み、ステップS4で生成した暗号キー80により暗号化パスワードを復号し、ステップS5で復号したパスワードと入力したパスワードを比較照合し、図5のステップS5にリターンして照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定することになる。

[0098] このためUSBキー26と暗号化媒体としてのMO媒体15の組み合わせにより、複数の記憶装置10に対し、データを持ち回りして利用する運用が可能である。

[0099] 図11はUSBキーからパスワードのみを入力する他の認証処理の説明図である。図11(A)の認証に必要な情報の保存状態にあっては、USBキー26にはパスワード74のみが保存されており、暗号化パスワード78はMO媒体15では記憶装置10に保存

されている。記憶装置10の暗号処理部72は図10の実施形態と同様、パスワード74から暗号キー80を生成する機能を備えている。

[0100] 図11(B)は図11(A)を対象とした認証処理のフローチャートである。この認証処理は、ステップS1でUSBキー26からパスワード74を読み込み、ステップS2で入力したパスワード74から記憶装置10の暗号処理部72が暗号キー80を生成する。

[0101] 続いてステップS3で生成した暗号キー80により暗号化パスワード78からパスワードを復号し、ステップS4で復号したパスワードと入力したパスワード74を比較照合し、図5のメインルーチンにリターンし、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定することになる。

[0102] 図12、図13及び図14は本発明の記憶装置10による制御処理の他の実施形態を示したフローチャートであり、この実施形態にあっては、暗号化媒体としてMOカートリッジ及びメモリカードの両方を対象として運用することを特徴とする。

[0103] 図12において、記憶装置10の電源を投入するとステップS1でUSBキー26の接続の有無をチェックし、USBキーの接続を判別するとステップS2でストレージ媒体としてのMOカートリッジ14及びメモリカード16の内容を確認した後、ステップS3で暗号化媒体か否かチェックする。この場合、MOカートリッジ14及びメモリカード16のいずれについても暗号化媒体と判別される。

[0104] 続いてステップS4で暗号キーに基づく認証処理を実行する。この認証処理の詳細は図8ー図11のいずれかの処理となる。ステップS5で認証成功が判別されると、ステップS6で暗号処理モードが設定され、認証失敗は図13のステップS20で通常モードが設定される。

[0105] ステップS6で暗号処理モードが設定されるとステップS7で、上位装置の接続をチェックし、ステップS8で周辺機器動作モードを設定する。接続がなければステップS14で単体動作モードの設定となる。

[0106] ステップS8の周辺機器動作モードにあっては、ステップS9でリードコマンドを判別すると、ステップS10でこのときアクセス対象となっているMOカートリッジまたはメモリカードの媒体から読み出した暗号化データを復号して上位装置に転送する。

[0107] またステップS11でライトコマンドを実施した場合にはステップS12で上位装置から

のデータを暗号化してMOカートリッジまたはメモリカードの媒体に書き込む。そしてこのステップS9ーS12の処理をステップS13で停止指示があるまで繰り返す。

[0108] ステップS14で単体動作モードが設定された場合には、ステップS15でコピー要求の有無をチェックし、コピー要求があればステップS16に進み次の処理を行う。

(1)コピー元となるMOカートリッジまたはメモリカードの内容のメニュー表示

(2)コピー元が暗号化データの場合は、そのままコピー転送。

(3)コピー元が通常データの場合は、暗号化してコピー転送。

[0109] 続いてステップS17で表示要求を判別するとステップS18に進み、MOカートリッジまたはメモリカードのメニューを表示し、選択したデータが暗号化データであればこれを復号して表示する。このステップS15からの処理はステップS19で停止指示があるまで繰り返す。

[0110] 図13のステップS20で通常モードが設定された場合にはステップS21ーS31の処理を行う。これは図6のステップS20ーS31の処理と基本的に同じである。また図13においてステップS21で上位装置の接続がなかった場合には図14のステップS32に進み、単体動作モードを設定する。図14のステップS32ーS44は図7のステップS32ーS44の処理と基本的に同じとなる。

[0111] 図15はリモートコントローラ24により暗号キー情報を入力する場合の制御処理のフローチャートである。図15において、記憶装置10の電源を投入すると、ステップS2でストレージ媒体の内容を確認した後、ステップS3で暗号化媒体か否かチェックし、暗号化媒体であればステップS4によりリモートコントローラ24から暗号キー情報を受信して認証処理を実行する。

[0112] この認証処理についてステップS5で認証成功を判別するとステップS6で暗号処理モードを設定する。一方、認証失敗であった場合にはステップS20で通常モードを設定する。ステップS6で暗号処理モードを設定した後の処理は図5のステップS7ーS19の処理と同じとなる。またステップS20で通常モードを設定した場合の処理は図6のステップS21ーS31及び図7のステップS32ーS44の処理と同じとなる。

[0113] ステップS4におけるリモートコントローラから暗号キー情報を受信した認証処理の詳細は、図8ー図11に示した認証処理において、USBキー26に保存しているパスワ

ード74や暗号キー76がリモートコントローラ24に格納されている点が相違し、その他は同じとなる。

[0114] またステップS4におけるリモートコントローラ24による暗号キー情報の送信は、リモートコントローラ24に設けている暗号キー送信用の操作釦を押すことで行う。また図10及び図11の認証処理のようにパスワード74のみを入力する場合には、リモートコントローラ24の釦操作でパスワードを送信して記憶装置10に受信入力するようにしても良い。

[0115] 図16は装置の操作部により暗号キー情報を入力する場合の制御処理のフローチャートである。この制御処理にあっては、ステップS2でストレージ媒体の内容確認を行った後、ステップS3で暗号化媒体か否かチェックし、暗号化媒体であった場合にはステップS4で図2(A)に示した記憶装置10の液晶ディスプレイ上にパスワードを入力するための入力画面を表示する。

[0116] この入力画面に対し操作部30の方向キー30−1ー30−4及び決定キー32を使用してパスワードを入力し、釦操作で入力したパスワードに基づく認証処理を行う。ステップS4の認証処理につきステップS5で認証成功が判別されるとステップS6の暗号処理モードの設定となり、ステップS6以降については図5のステップS7ーS19と同じ処理となる。

[0117] また認証に失敗した場合にはステップS20で通常モードが設定され、この場合には図6のステップS21ーS31及び図7のステップS32ーS44と同じ処理を行う。

[0118] この図16の装置操作部を使用した暗号キー情報の入力については、パスワードと暗号キーの両方を入力することは操作が煩雑になることから、パスワードのみの入力で認証を行う図10または図11の認証処理とすることが望ましい。

[0119] また図16の制御処理のように装置操作部の釦操作で暗号キー情報、すなわちパスワードや暗号キーを入力する記憶装置10とした場合には、暗号化動作モードか通常モードかの設定はユーザが動作モードを選択できるようにしてもよい。

[0120] 更に本発明の記憶装置10としては図4のようにメインプロセッサ54に設けているリアルタイムクロック58に基づきユーザが任意に設定した時刻またはインターバルで自動的にログファイルやタイムスタンプをもったフォルダを作成し、ホスト12のログやホス

ト12から送られてくるデータを時刻単位で保存管理する日時管理処理を行う。

[0121] このような日時管理処理によりホスト12の動作履歴や一定時間中に処理されたデータを自動的にバックアップする用途に用いることができる。このホスト12と履歴データの電源に対しては別途ホスト12側にシンクロナイド機能を持たせた連携アプリケーションを設けることになる。

[0122] 尚、上記の実施形態は記憶装置の記憶デバイスとしてMOドライブとメモリカードコントローラを例にとるものであったが、これ以外にハードディスクドライブ(HDD)や適宜の記憶ドライブを設けるようにしてもよい。

[0123] またホストとの入出力処理を行うインターフェース専用のサブプロセッサとしてIEEE1394USBを例にとるものであったが、これ以外にワイヤレスのインタフェースを用いてもよいし、さらに必要に応じて適宜のインタフェース用プロセッサ(LSI)を用いることができる。

[0124] 更に上記の実施形態は、USBキー26にパスワードと暗号キー、又はパスワードのみを格納した場合を例にとるものであったが、暗号キーのみを格納するようにしてもよい。USBキー26に暗号キーのみを格納した場合には、装置固有のマジックナンバーを暗号化した暗号化マジックナンバーを媒体又は装置に予め登録しておき、暗号キーにより暗号化マジックナンバーを復号して装置固有のマジックナンバーと比較することで認証照合を行えば良い。

[0125] また本発明はその目的と利点を損なうことのない適宜の変形を含み、更に上記の実施形態に示した数値による限定は受けない。

[0126] 更に本発明は記憶装置のコンピュータ、具体的にはメインプロセッサ54で実行されるプログラムを提供するものであり、このプログラムは図5ー図7、図8(B)、図9(B)、図10(B)、図11(B)及び図12ー図16のフローチャートに示した内容を持つことになる。

請求の範囲

[1] 上位装置とのデータの入出力がなされ、前記データを処理するインタフェース処理部を備えた記憶装置に於いて、

着脱自在な第1記憶媒体のデータの読み出し又は書き込みを行う第1記憶媒体処理部と、

着脱自在な第2記憶媒体のデータの読み出し又は書き込みを行う第2記憶媒体処理部と、

暗号キー情報が前記上位装置を介さず該記憶装置に直接入力される暗号キー入力部と、

前記暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する暗号処理部と、

を備えたことを特徴とする記憶装置。

[2] 請求項1記載の記憶装置に於いて、前記暗号処理部は、前記暗号処理モードを設定した際に、前記上位装置又は前記第2記憶媒体からのデータを前記暗号キー情報に基づいて暗号化データに変換して前記第1記憶媒体に記憶する、または前記第1記憶媒体からの暗号化データを前記暗号キー情報に基づいて復号して前記上位装置、第2記憶媒体又は自己のディスプレイに転送することを特徴とする記憶装置。

[3] 請求項1記載の記憶装置に於いて、前記暗号処理部は、前記暗号処理モードを設定した際に、前記上位装置から受信した暗号化データを前記暗号キー情報に基づいて更に暗号化して2重暗号化データに変換して前記第1記憶媒体に記憶し、前記第1記憶媒体から前記上位装置に転送する2重暗号化データを前記暗号キー情報に基づいて前記暗号化データに復号することを特徴とする記憶装置。

[4] 請求項1記載の記憶装置に於いて、前記暗号キー入力部はUSBポートを備えたUSBインタフェースであり、前記USBポートに接続したUSBキーに記憶された前記暗号キー情報を読み出して前記暗号処理部に入力することを特徴とする記憶装置。

[5] 請求項1記載の記憶装置に於いて、前記暗号キー入力部は赤外線受信部であり、リモートコントローラから赤外線により送信された前記暗号キー情報を受信して前記暗号処理部に入力することを特徴とする記憶装置。

[6] 請求項1記載の記憶装置に於いて、前記暗号キー入力部はユーザ操作部であり、操作入力された前記暗号キー情報を前記暗号処理部に転送することを特徴とする記憶装置。

[7] 請求項1記載の記憶装置に於いて、前記暗号キー入力部は、前記暗号キー情報としてパスワードと暗号キーを入力し、

前記暗号処理部は、前記暗号キーにより予め保存された暗号化パスワードを復元して入力パスワードと比較し、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定することを特徴とする記憶装置。

[8] 請求項1記載の記憶装置に於いて、前記暗号キー入力部は、前記暗号キー情報としてパスワードを入力し、

前記暗号処理部は、前記パスワードから暗号キーを生成して予め保存された暗号化パスワードを復元して入力パスワードと比較し、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定することを特徴とする記憶装置。

[9] 請求項1記載の記憶装置に於いて、前記暗号処理部は、前記暗号キー情報が存在しない場合は、前記第1記憶媒体又は第2記憶媒体からの暗号化データの読出要求に対し前記表示処理部により暗号キー情報の入力を要求するエラーメッセージを表示させることを特徴とする記憶装置。

[10] 請求項1記載の記憶装置に於いて、前記暗号処理部は、前記暗号キー情報が存在しない場合は、前記第1記憶媒体又は第2記憶媒体からの暗号化データの読出要

求に対し読み出しを禁止して前記暗号化データの存在を隠蔽することを特徴とする記憶装置。

[11] 請求項10記載の記憶装置に於いて、前記暗号処理部は、前記暗号キー情報が存在しない場合は、前記第1記憶媒体又は第2記憶媒体に格納したファイルメニューに非暗号化データのみを表示し、前記暗号化データの存在を隠蔽することを特徴とする記憶装置。

[12] 上位装置とのデータの入出力がなされ、前記データを処理するインタフェース処理部を備えた記憶装置の制御方法に於いて、

着脱自在な第1記憶媒体のデータの読み出し又は書き込みを行う第1記憶媒体処理ステップと、

着脱自在な第2記憶媒体のデータの読み出し又は書き込みを行う第2記憶媒体処理ステップと、

暗号キー情報が前記上位装置を介さずに該記憶装置に直接入力される暗号キー入力ステップと、

前記暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する暗号処理ステップと、

を備えたことを特徴とする記憶装置の制御方法。

[13] 請求項12記載の記憶装置の制御方法に於いて、前記暗号処理ステップは、前記暗号処理モードを設定した際に、前記上位装置又は前記第2記憶媒体からのデータを前記暗号キー情報に基づいて暗号化データに変換して前記第1記憶媒体に記憶する、または前記第1記憶媒体からの暗号化データを前記暗号キー情報に基づいて復号して前記上位装置、第2記憶媒体又は該記憶装置のディスプレイに転送することを特徴とする記憶装置の制御方法。

[14] 請求項12記載の記憶装置の制御方法に於いて、前記暗号処理ステップは、前記

暗号処理モードを設定した際に、前記上位装置から受信した暗号化データを前記暗号キー情報に基づいて更に暗号化して2重暗号化データに変換して前記第1記憶媒体に記憶し、前記第1記憶媒体から前記上位装置に転送する2重暗号化データを前記暗号キー情報に基づいて前記暗号化データに復号することを特徴とする記憶装置の制御方法。

[15] 請求項12記載の記憶装置の制御方法に於いて、前記暗号キー入力ステップは、USBポートに接続したUSBキーに記憶された前記暗号キー情報を読み出して入力することを特徴とする記憶装置の制御方法。

[16] 請求項12記載の記憶装置の制御方法に於いて、前記暗号キー入力ステップは、リモートコントローラから赤外線により送信された前記暗号キー情報を受信して入力することを特徴とする記憶装置の制御方法。

[17] 請求項12記載の記憶装置の制御方法に於いて、前記暗号キー入力ステップはユーザ操作部の操作による前記暗号キー情報を入力することを特徴とする記憶装置の制御方法。

[18] 請求項12記載の記憶装置の制御方法に於いて、前記暗号キー入力ステップは、前記暗号キー情報としてパスワードと暗号キーを入力し、

前記暗号処理ステップは、前記暗号キーにより予め保存された暗号パスワードを復元して入力パスワードと比較し、照合成功で暗号処理モードを設定し、照合失敗で通常モードを設定することを特徴とする記憶装置の制御方法。

[19] 上位装置とのデータの入出力がなされ、前記データを処理するインタフェース処理部を備えた記憶装置のコンピュータに、

着脱自在な第1記憶媒体のデータの読み出し又は書き込みを行う第1記憶媒体処

理ステップと、

着脱自在な第2記憶媒体のデータの読み出し又は書き込みを行う第2記憶媒体処理ステップと、

暗号キー情報が前記上位装置を介さずに該記憶装置に直接入力される暗号キー入力ステップと、

前記暗号キー入力部からの暗号キー情報の入力に基づいて暗号処理モードが設定され、データの暗号化又は復号化を実行する暗号処理ステップと、

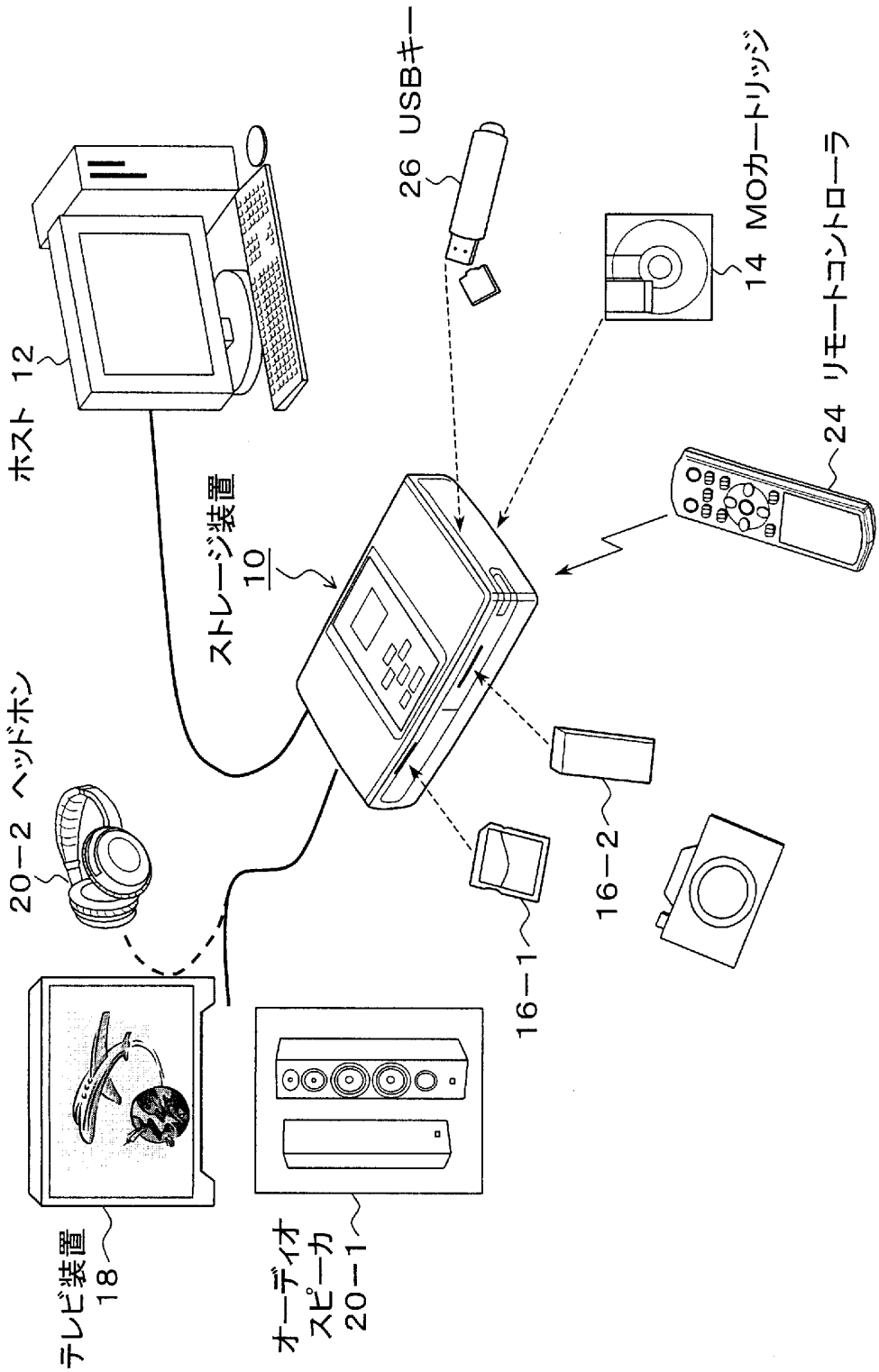
を実行させることを特徴とするプログラム。

ータの暗号化又は復号化を実行する暗号処理ステップと、

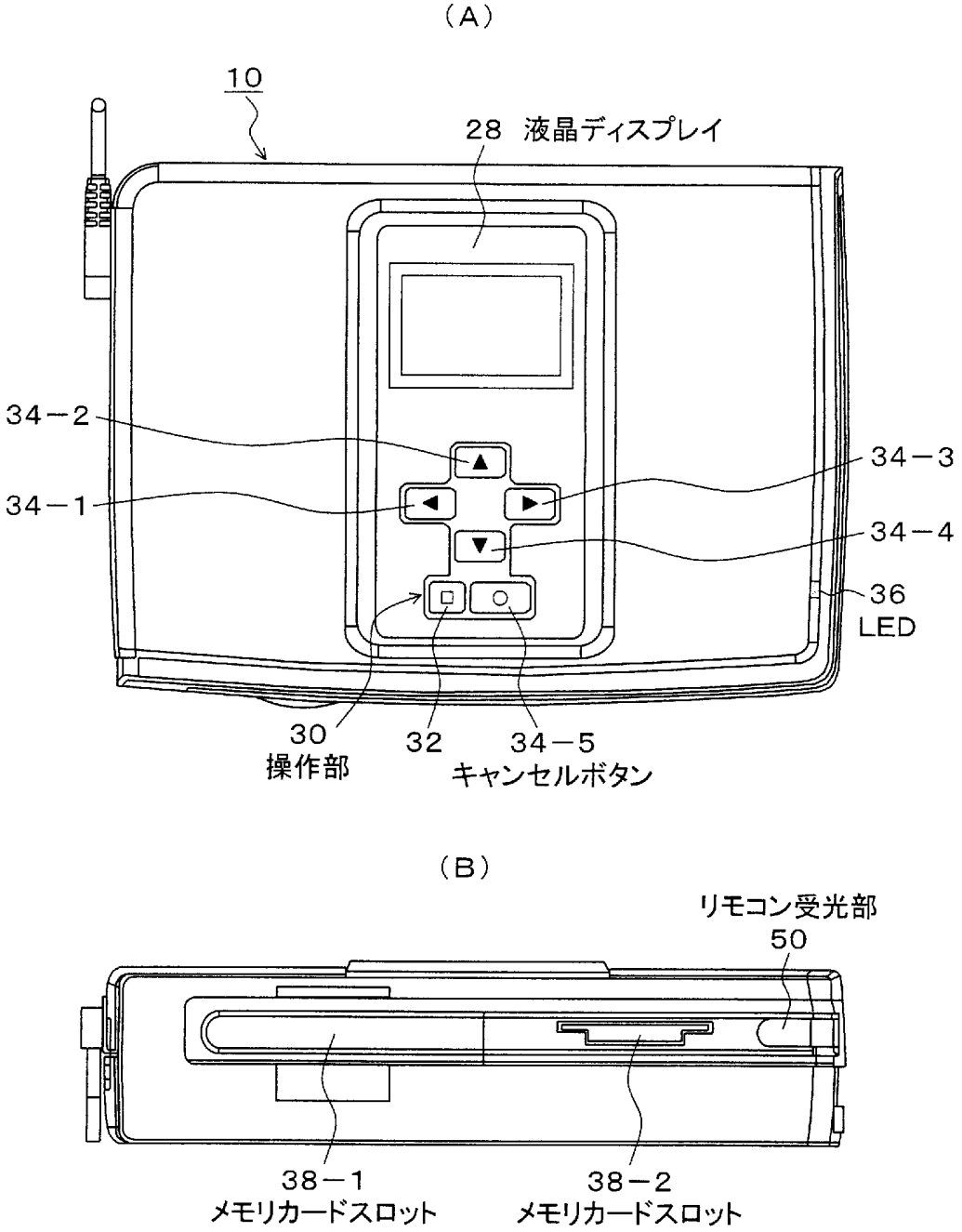
を実行させることを特徴とするプログラム。

[20] 請求項19記載のプログラムに於いて、前記暗号処理ステップは、前記暗号処理モードを設定した際に、前記上位装置又は前記第2記憶媒体からのデータを前記暗号キー情報に基づいて暗号化データに変換して前記第1記憶媒体に記憶する、または、前記第1記憶媒体からの暗号化データを前記暗号キー情報に基づいて復号して前記上位装置、第2記憶媒体又は該記憶装置のディスプレイに転送することを特徴とするプログラム。

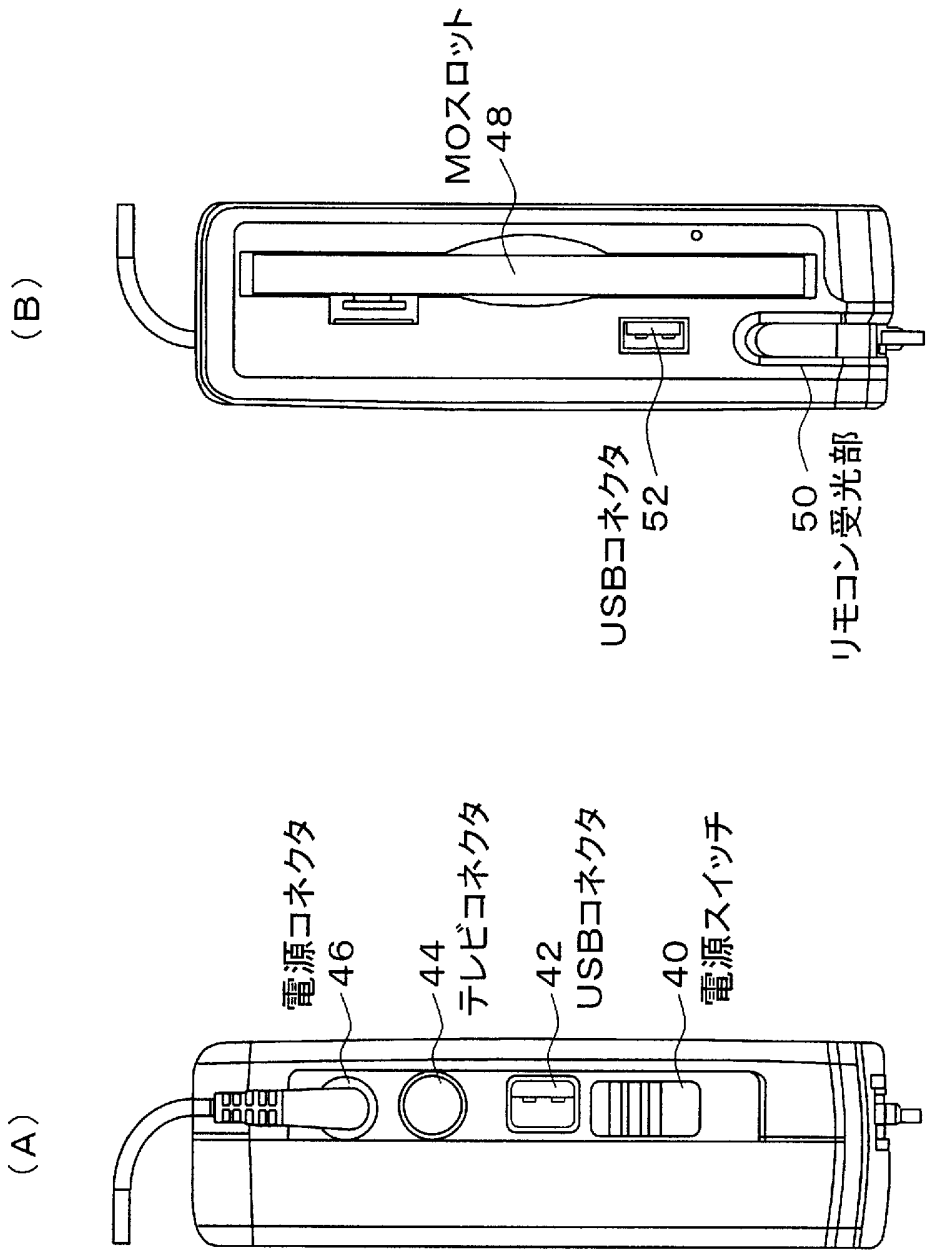
[図1]


ホスト 12
26 USBキー
14 MOカートリッジ
24 リモートコントローラ
ストレージ装置
10
20−2 ヘッドホン
16−2
16−1
テレビ装置
18
オーディオ
スピーカ
20−1

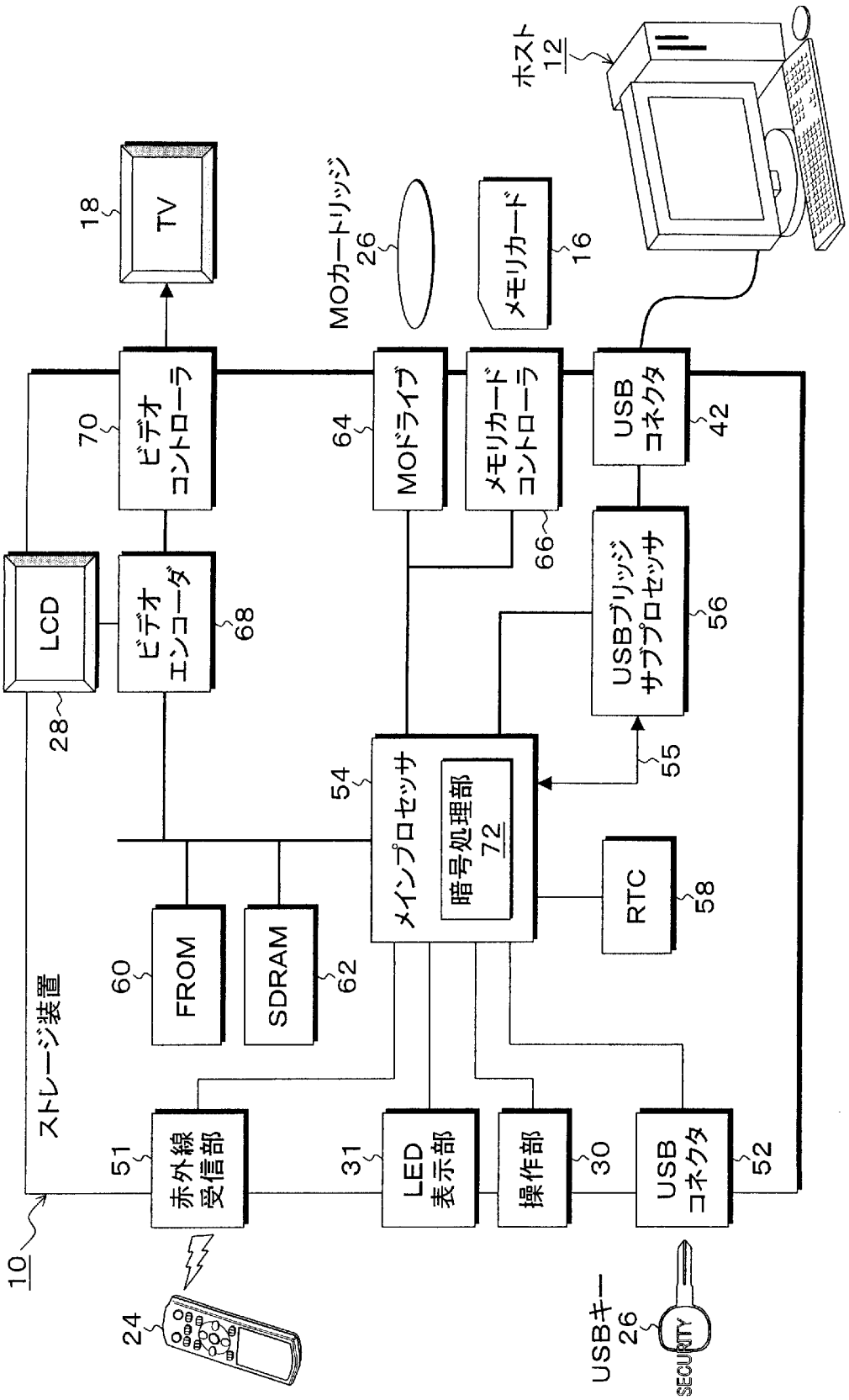
[図2]


（A）
10
28 液晶ディスプレイ
34－2
34－1
34－3
34－4
36
LED
30
操作部
32
34－5
キャンセルボタン
（B）
リモコン受光部
50
38－1
メモリカードスロット
38－2
メモリカードスロット

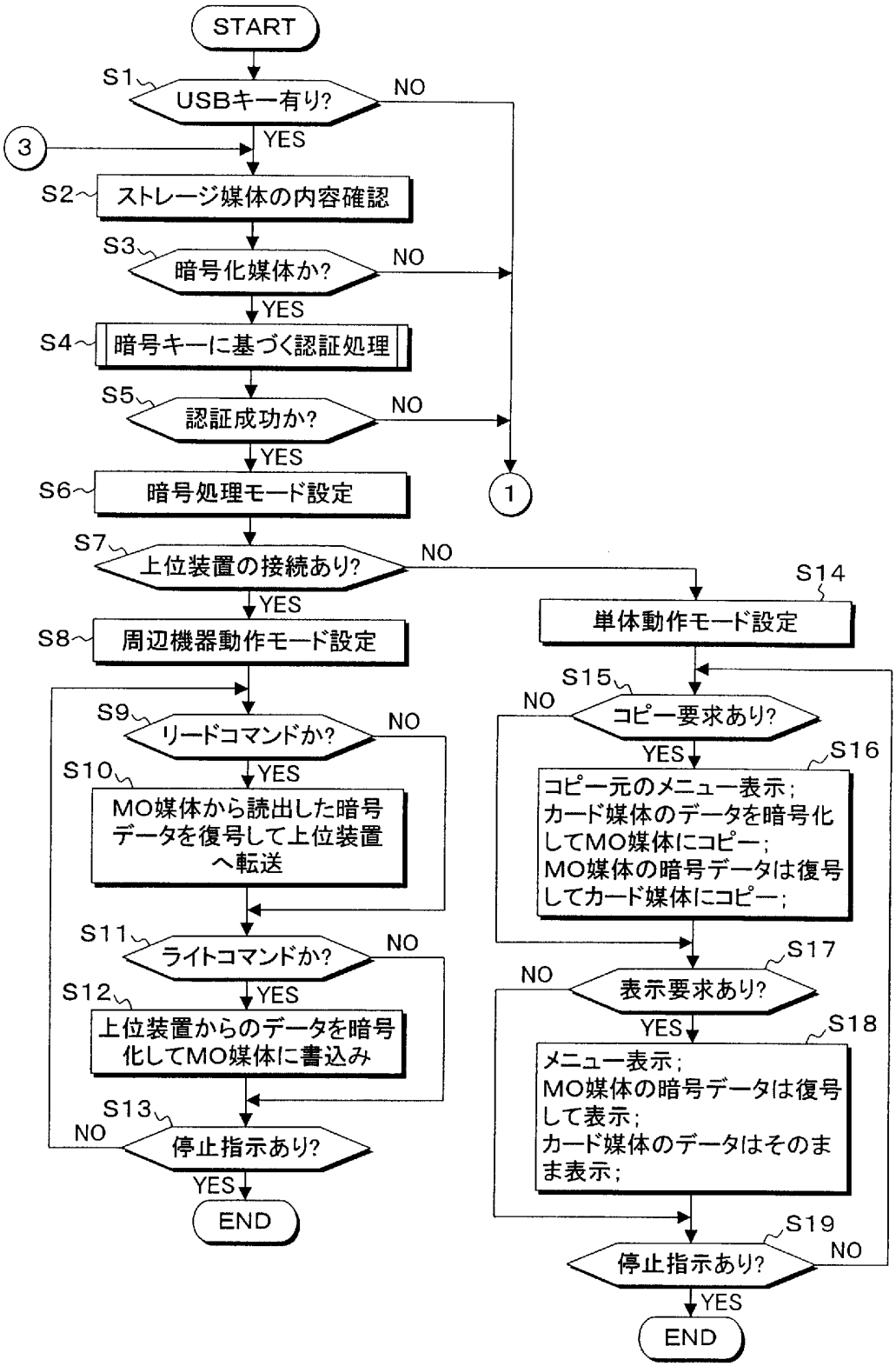
[図3]


(B)
MOスロット
48
USBコネクタ
52
50
リモコン受光部
(A)
電源コネクタ
46
44
テレビコネクタ
42
USBコネクタ
40
電源スイッチ

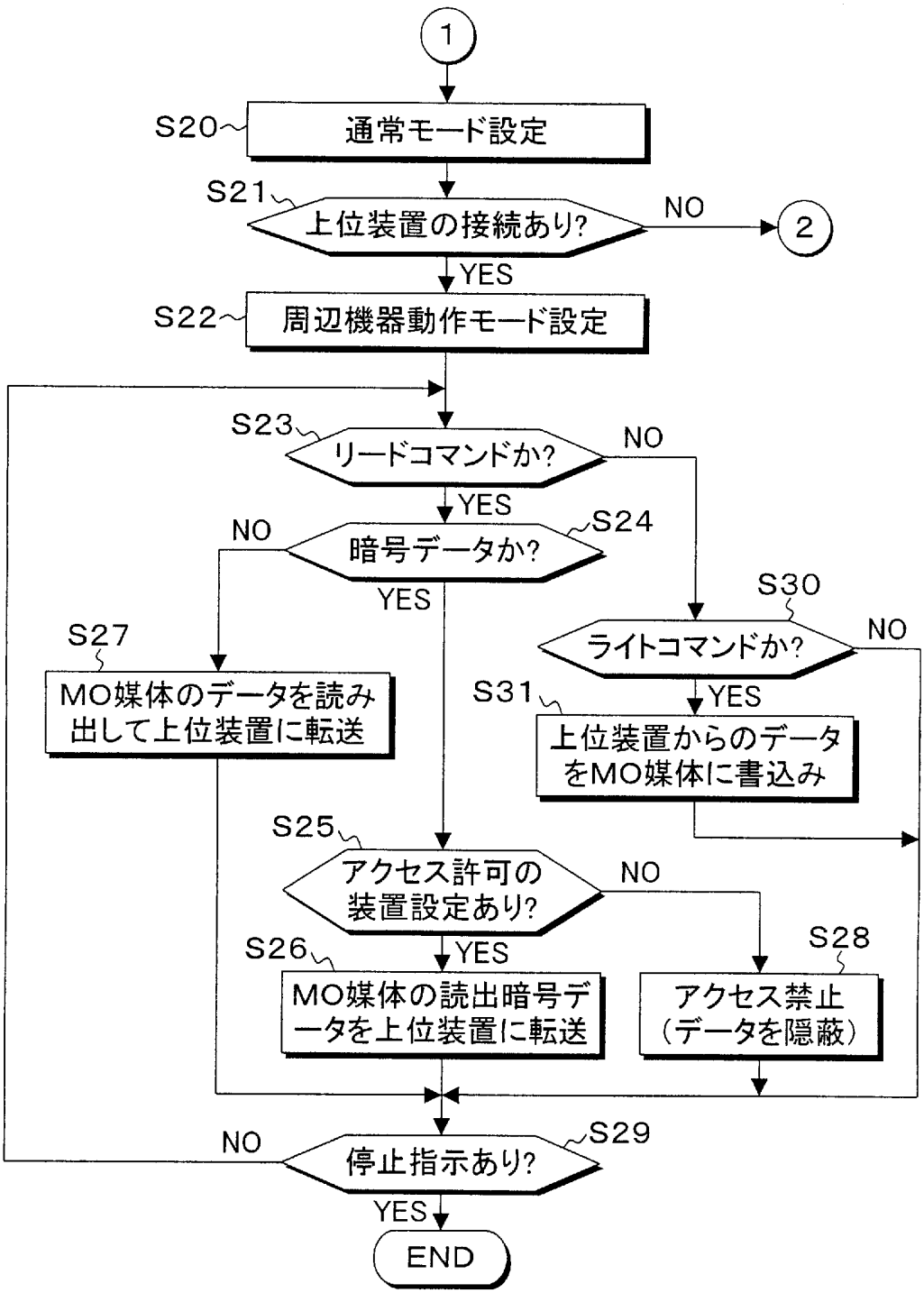
[図4]


ホスト
12
18
TV
MOカートリッジ
26
メモリカード
16
70
ビデオ
コントローラ
64
MOドライブ
メモリカード
コントローラ
66
USB
コネクタ
42
LCD
28
ビデオ
エンコーダ
68
USBブリッジ
サブプロセッサ
56
54
メインプロセッサ
暗号処理部
72
55
RTC
58
60
FROM
SDRAM
62
ストレージ装置
51
赤外線
受信部
31
LED
表示部
操作部
30
USB
コネクタ
52
10
24
USBキー
26
SECURITY

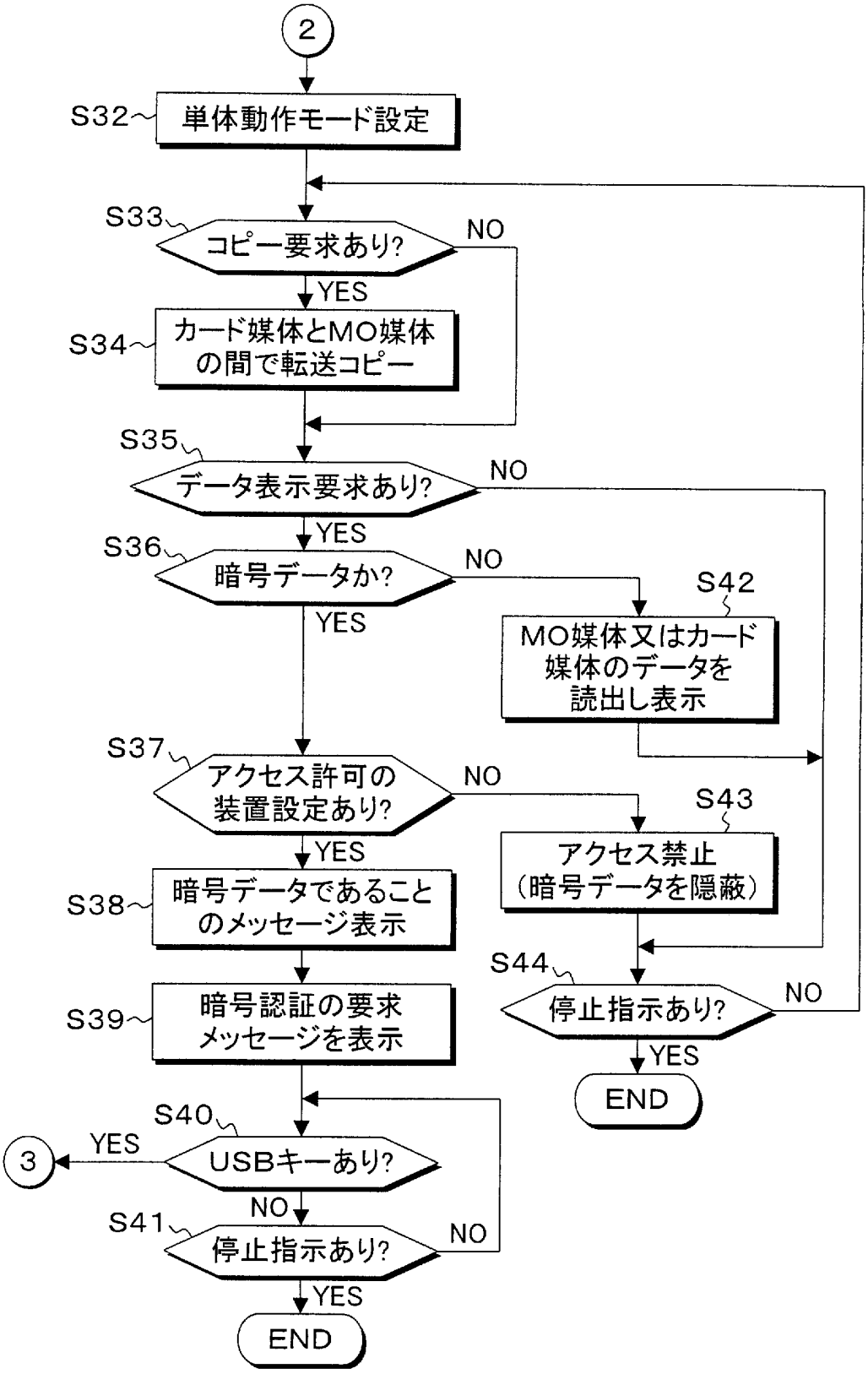
[図5]


START
S1
USBキー有り?
NO
YES
3
S2
ストレージ媒体の内容確認
S3
暗号化媒体か?
NO
YES
S4
暗号キーに基づく認証処理
S5
認証成功か?
NO
YES
1
S6
暗号処理モード設定
S7
上位装置の接続あり?
NO
YES
S8
周辺機器動作モード設定
S9
リードコマンドか?
NO
YES
S10
MO媒体から読出した暗号データを復号して上位装置へ転送
S11
ライトコマンドか?
NO
YES
S12
上位装置からのデータを暗号化してMO媒体に書込み
S13
停止指示あり?
NO
YES
END
S14
単体動作モード設定
S15
コピー要求あり?
NO
YES
S16
コピー元のメニュー表示;
カード媒体のデータを暗号化してMO媒体にコピー;
MO媒体の暗号データは復号してカード媒体にコピー;
S17
表示要求あり?
NO
YES
S18
メニュー表示;
MO媒体の暗号データは復号して表示;
カード媒体のデータはそのまま表示;
S19
停止指示あり?
NO
YES
END

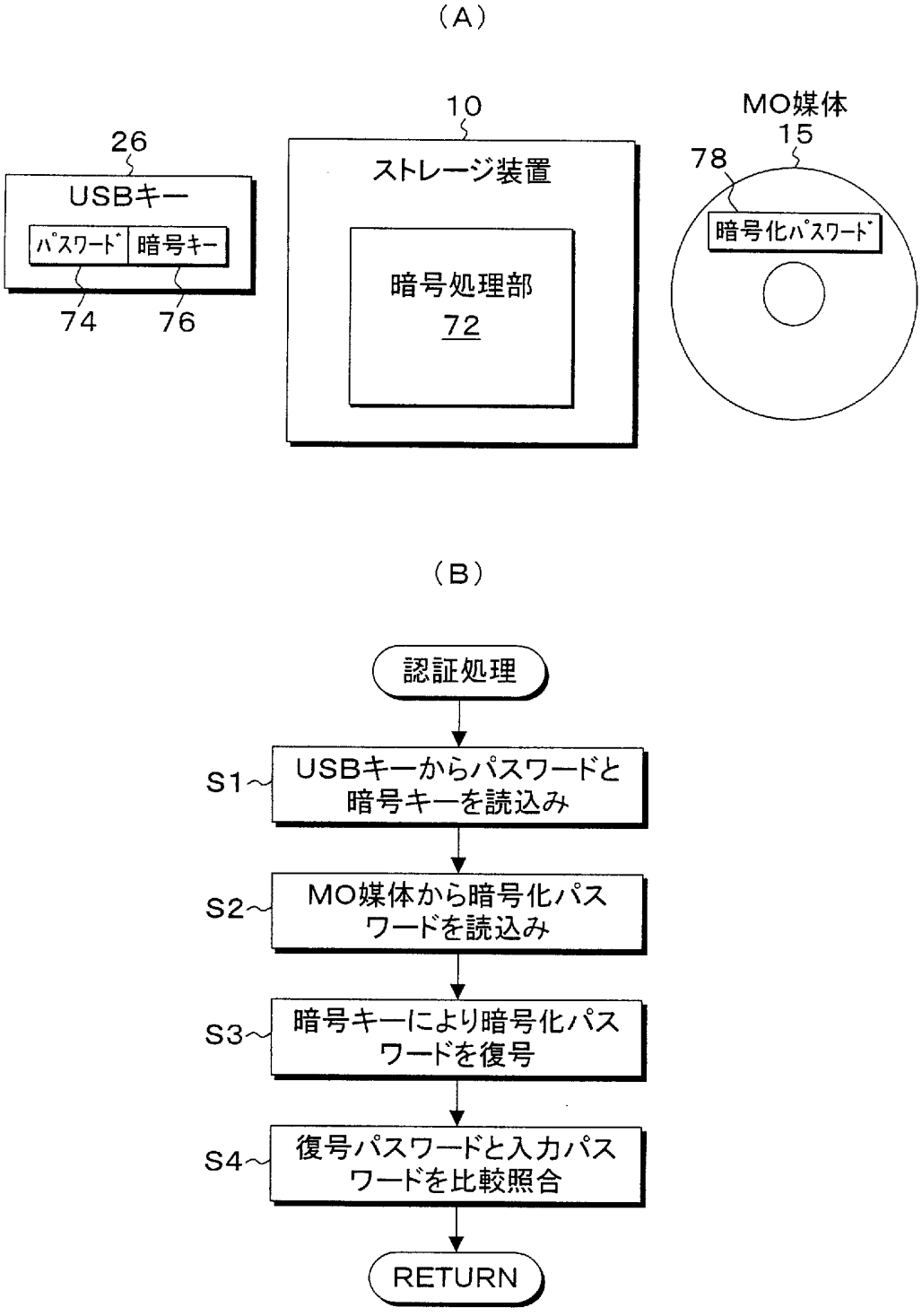
[図6]


1
S20
通常モード設定
S21
上位装置の接続あり?
NO
2
YES
S22
周辺機器動作モード設定
S23
リードコマンドか?
NO
YES
NO
S24
暗号データか?
YES
S30
ライトコマンドか?
NO
S27
MO媒体のデータを読み出して上位装置に転送
YES
S31
上位装置からのデータをMO媒体に書込み
S25
アクセス許可の装置設定あり?
NO
S26
YES
S28
MO媒体の読出暗号データを上位装置に転送
アクセス禁止（データを隠蔽）
NO
S29
停止指示あり?
YES
END

[図7]

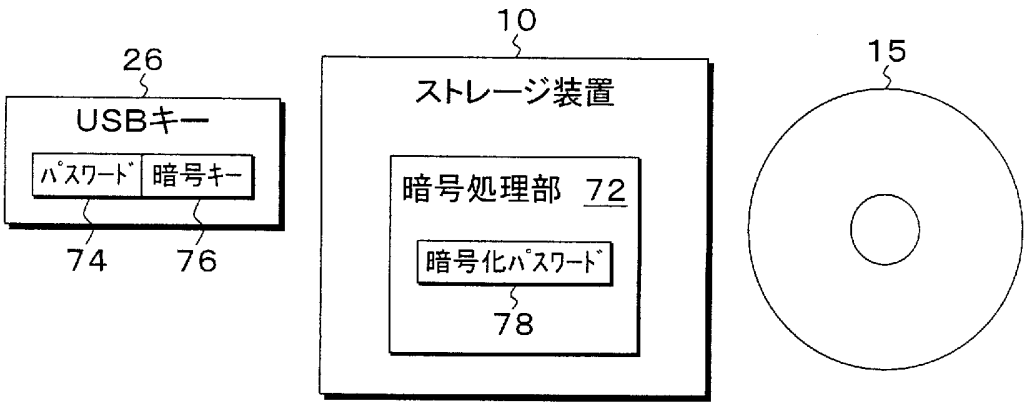

2
S32
単体動作モード設定
S33
コピー要求あり?
NO
YES
S34
カード媒体とMO媒体の間で転送コピー
S35
データ表示要求あり?
NO
YES
S36
暗号データか?
NO
YES
S42
MO媒体又はカード媒体のデータを読出し表示
S37
アクセス許可の装置設定あり?
NO
YES
S43
アクセス禁止（暗号データを隠蔽）
S38
暗号データであることのメッセージ表示
S44
停止指示あり?
NO
YES
END
S39
暗号認証の要求メッセージを表示
S40
3
YES
USBキーあり?
NO
S41
停止指示あり?
NO
YES
END

[図8]

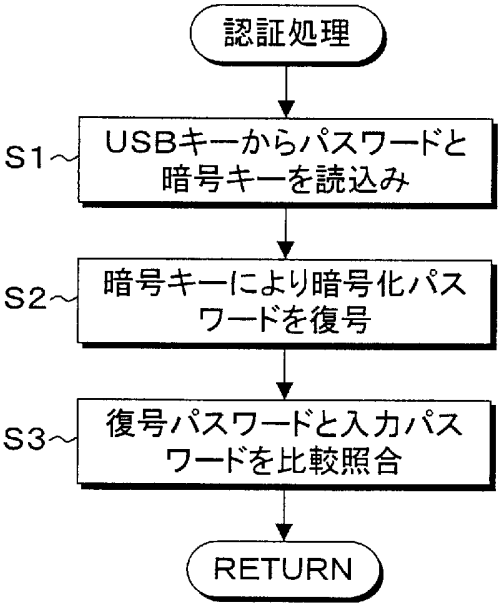

(A)
26
USBキー
ﾊﾟｽﾜｰﾄﾞ
暗号キー
74
76
10
ストレージ装置
暗号処理部
72
MO媒体
15
78
暗号化ﾊﾟｽﾜｰﾄﾞ
(B)
認証処理
S1
USBキーからパスワードと暗号キーを読込み
S2
MO媒体から暗号化パスワードを読込み
S3
暗号キーにより暗号化パスワードを復号
S4
復号パスワードと入力パスワードを比較照合
RETURN

[図9]

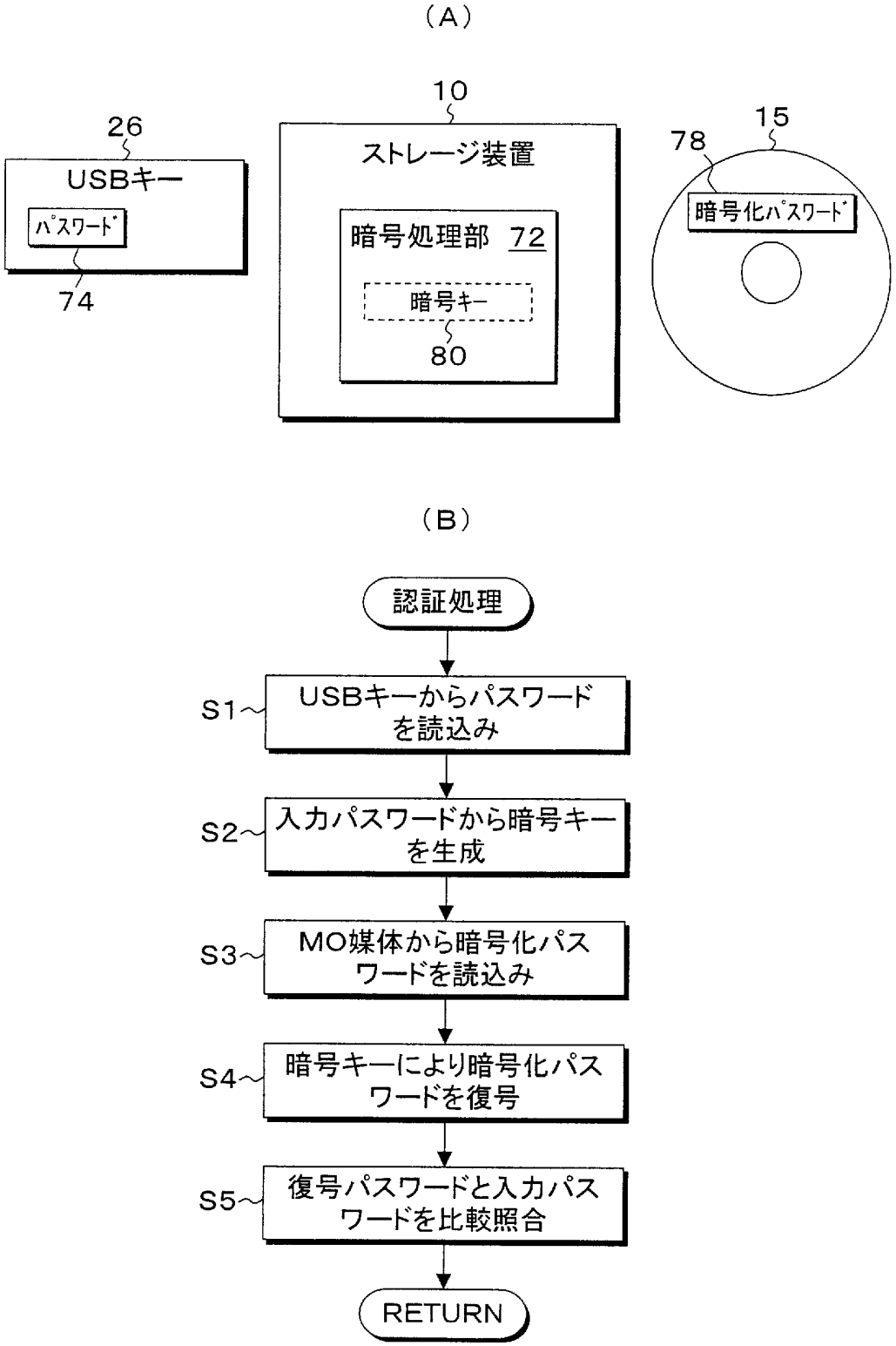
（A）


26
USBキー
ﾊﾟｽﾜｰﾄﾞ
暗号キー
74
76
10
ストレージ装置
暗号処理部 72
暗号化ﾊﾟｽﾜｰﾄﾞ
78
15

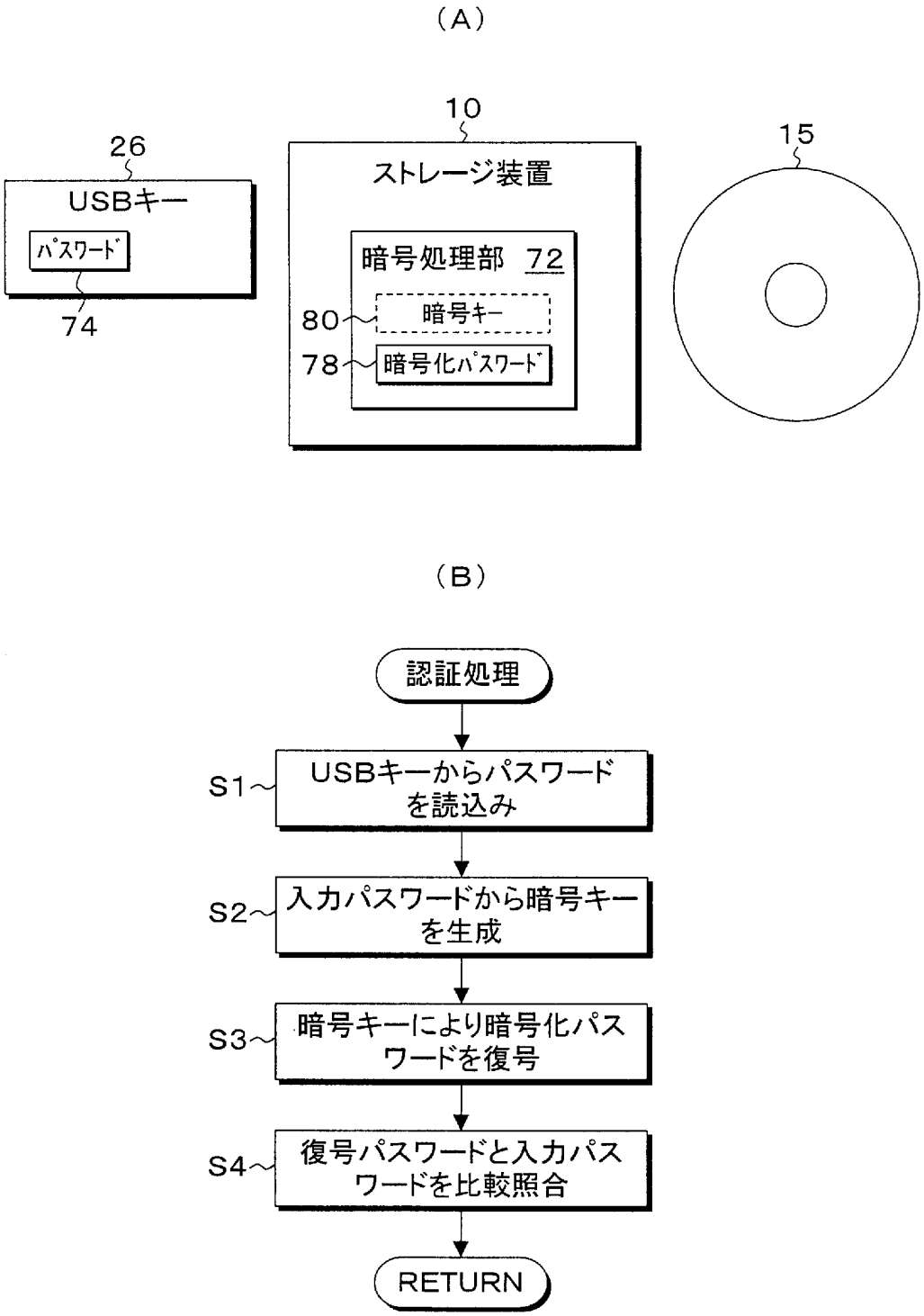
（B）


認証処理
S1
USBキーからパスワードと暗号キーを読込み
S2
暗号キーにより暗号化パスワードを復号
S3
復号パスワードと入力パスワードを比較照合
RETURN

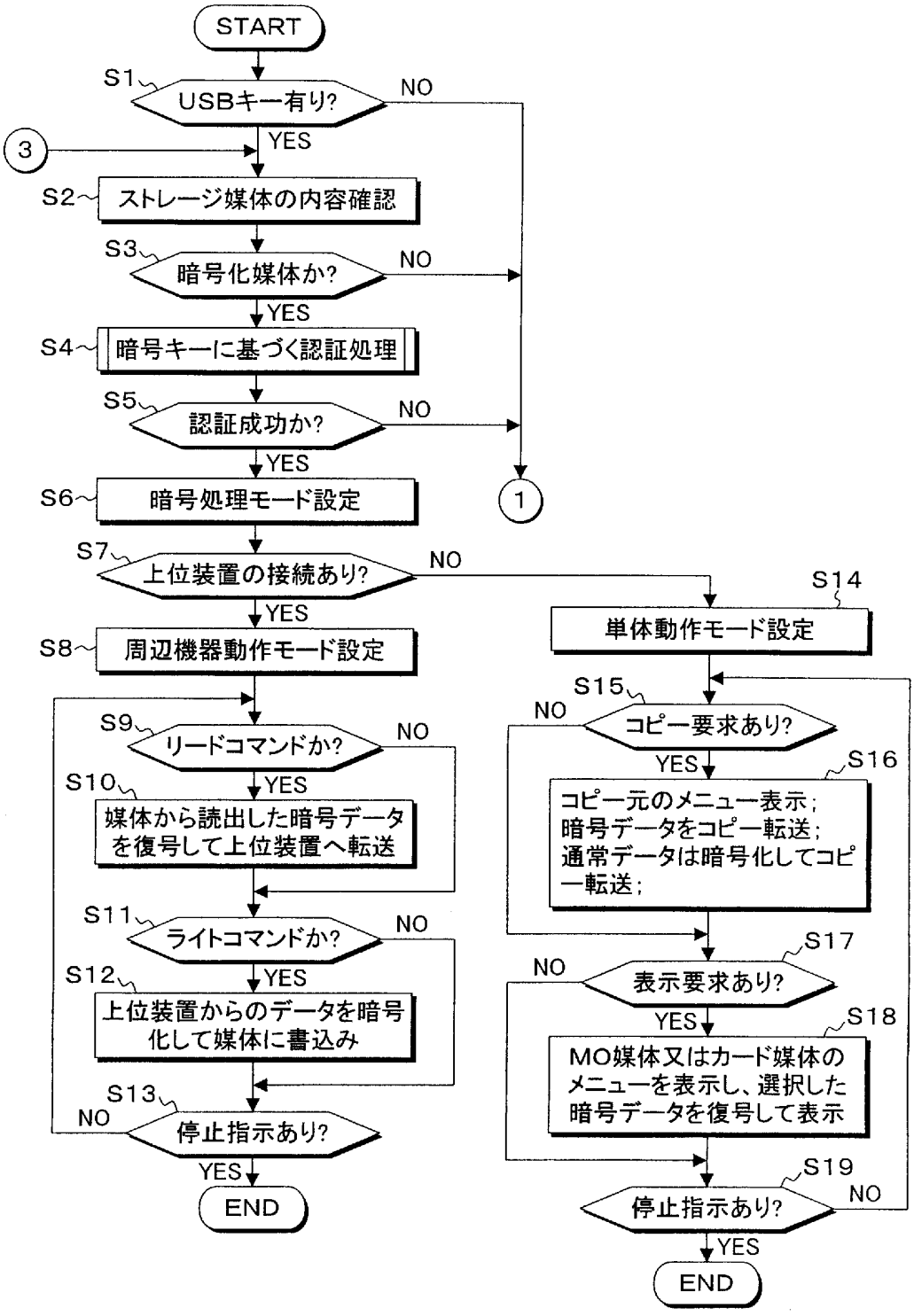
[図10]


(A)
10
ストレージ装置
暗号処理部 72
暗号キー
80
26
USBキー
ﾊﾟｽﾜｰﾄﾞ
74
15
78
暗号化ﾊﾟｽﾜｰﾄﾞ
(B)
認証処理
S1
USBキーからパスワード
を読込み
S2
入力パスワードから暗号キー
を生成
S3
MO媒体から暗号化パス
ワードを読込み
S4
暗号キーにより暗号化パス
ワードを復号
S5
復号パスワードと入力パス
ワードを比較照合
RETURN

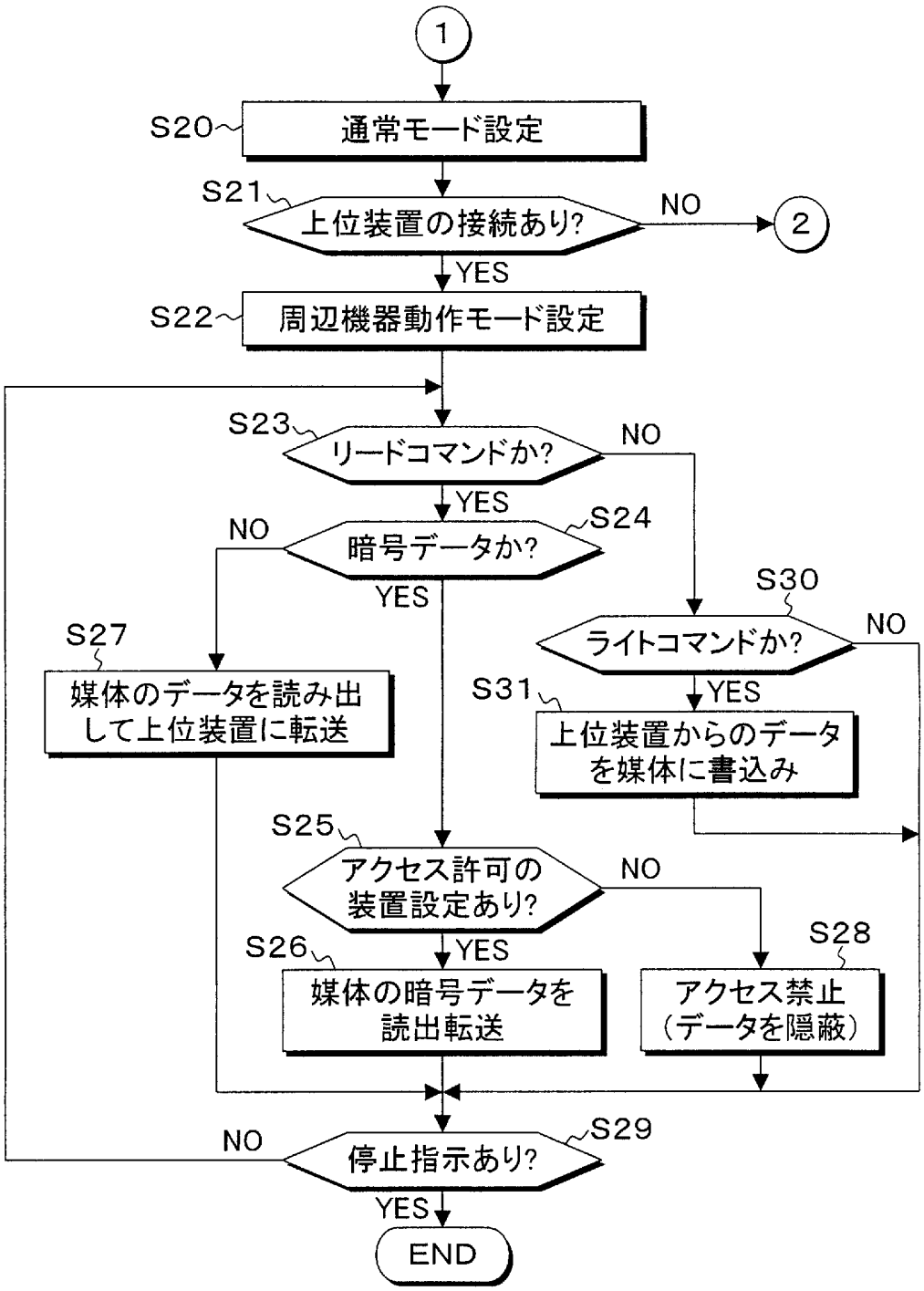
[図11]


(A)
10
26
USBキー
パスワード
74
ストレージ装置
暗号処理部 72
80
暗号キー
78
暗号化パスワード
15
(B)
認証処理
S1
USBキーからパスワードを読込み
S2
入力パスワードから暗号キーを生成
S3
暗号キーにより暗号化パスワードを復号
S4
復号パスワードと入力パスワードを比較照合
RETURN

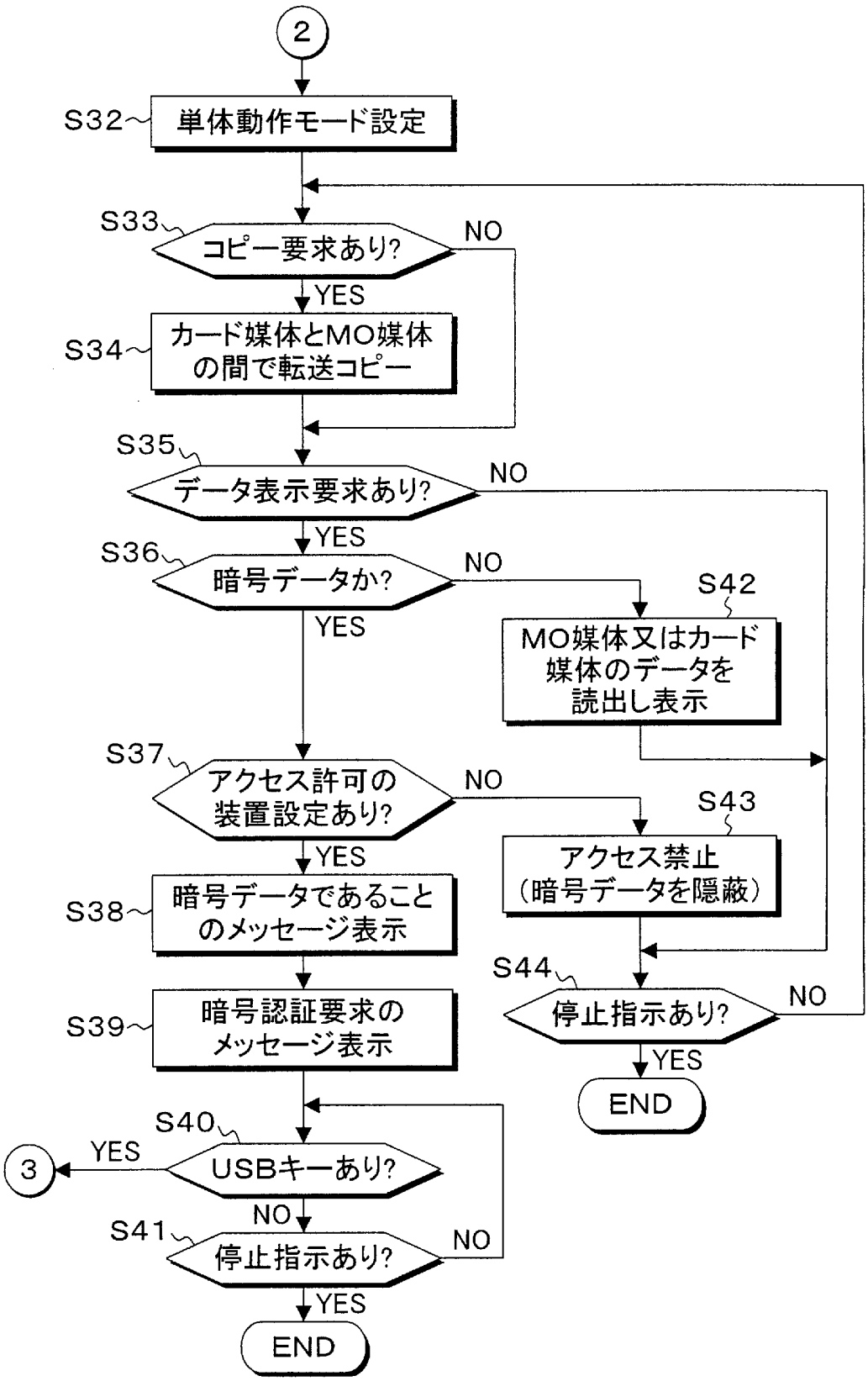
[図12]


START
S1
USBキー有り?
NO
YES
3
S2
ストレージ媒体の内容確認
S3
暗号化媒体か?
NO
YES
S4
暗号キーに基づく認証処理
S5
認証成功か?
NO
YES
1
S6
暗号処理モード設定
S7
上位装置の接続あり?
NO
YES
S8
周辺機器動作モード設定
S9
リードコマンドか?
NO
YES
S10
媒体から読出した暗号データを復号して上位装置へ転送
S11
ライトコマンドか?
NO
YES
S12
上位装置からのデータを暗号化して媒体に書込み
S13
停止指示あり?
NO
YES
END
S14
単体動作モード設定
S15
コピー要求あり?
NO
YES
S16
コピー元のメニュー表示;
暗号データをコピー転送;
通常データは暗号化してコピー転送;
S17
表示要求あり?
NO
YES
S18
MO媒体又はカード媒体のメニューを表示し、選択した暗号データを復号して表示
S19
停止指示あり?
NO
YES
END

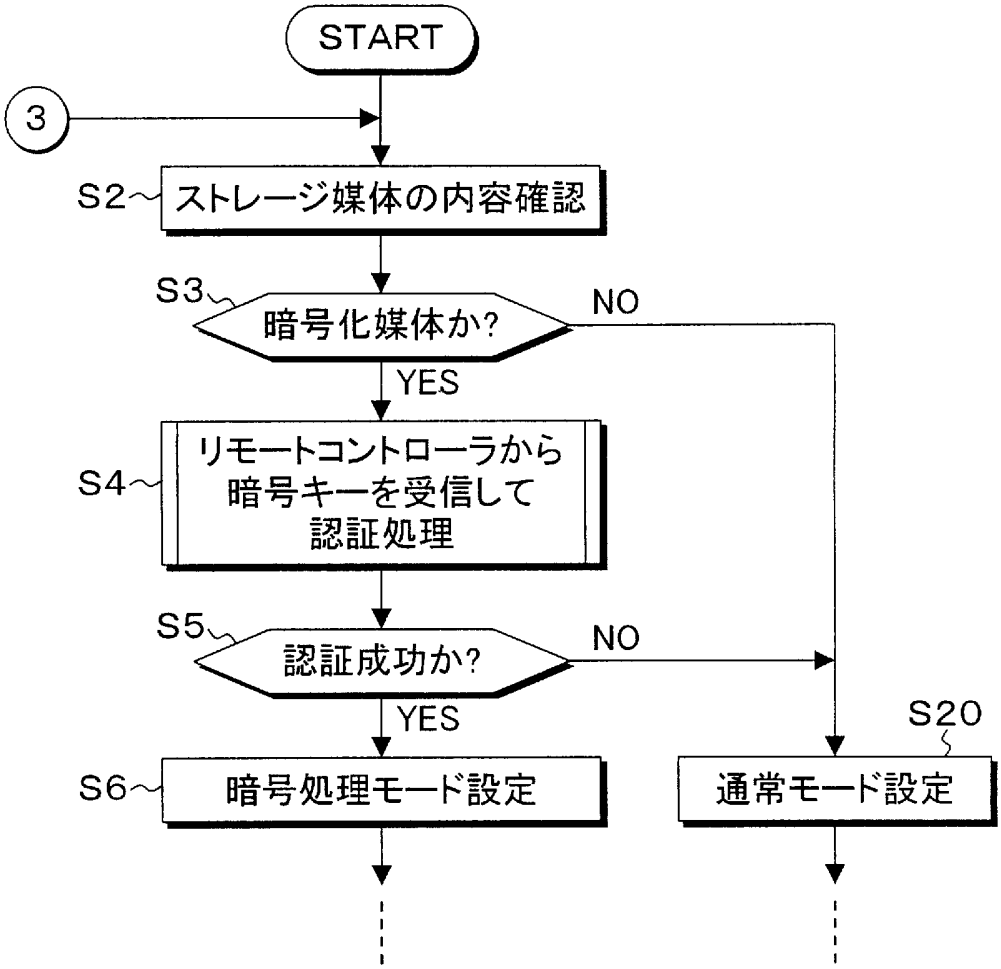
[図13]


1
S20
通常モード設定
S21
上位装置の接続あり?
NO
2
YES
S22
周辺機器動作モード設定
S23
リードコマンドか?
NO
YES
NO
S24
暗号データか?
YES
S30
ライトコマンドか?
NO
S27
媒体のデータを読み出して上位装置に転送
S31
YES
上位装置からのデータを媒体に書込み
S25
アクセス許可の装置設定あり?
NO
S26
YES
S28
媒体の暗号データを読出転送
アクセス禁止（データを隠蔽）
NO
S29
停止指示あり?
YES
END

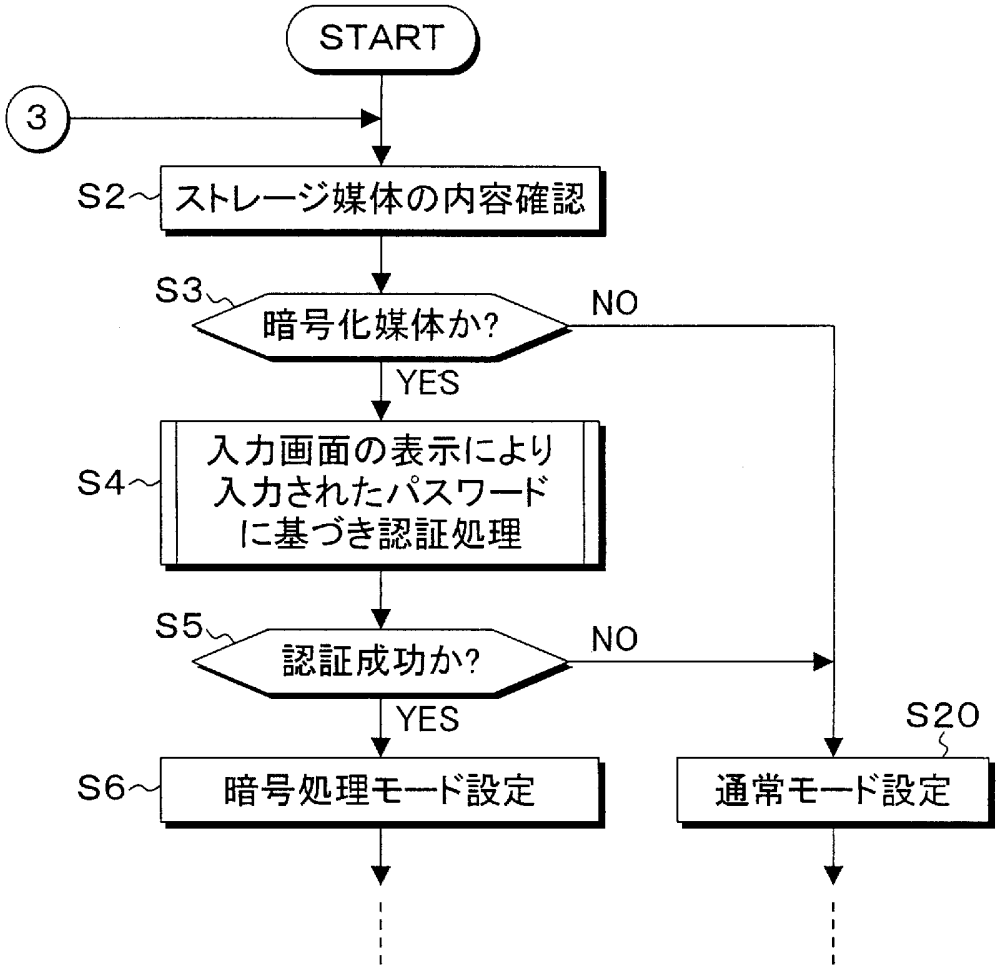
[図14]


2
S32
単体動作モード設定
S33
コピー要求あり?
NO
YES
S34
カード媒体とMO媒体の間で転送コピー
S35
データ表示要求あり?
NO
YES
S36
暗号データか?
NO
YES
S42
MO媒体又はカード媒体のデータを読出し表示
S37
アクセス許可の装置設定あり?
NO
YES
S43
アクセス禁止(暗号データを隠蔽)
S38
暗号データであることのメッセージ表示
S44
停止指示あり?
NO
YES
END
S39
暗号認証要求のメッセージ表示
S40
3
YES
USBキーあり?
NO
S41
停止指示あり?
NO
YES
END

[図15]


START
3
S2
ストレージ媒体の内容確認
S3
暗号化媒体か?
NO
YES
S4
リモートコントローラから
暗号キーを受信して
認証処理
S5
認証成功か?
NO
YES
S6
暗号処理モード設定
S20
通常モード設定

[図16]


START
3
S2
ストレージ媒体の内容確認
S3
暗号化媒体か?
NO
YES
S4
入力画面の表示により
入力されたパスワード
に基づき認証処理
S5
認証成功か?
NO
YES
S20
S6
暗号処理モード設定
通常モード設定

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/003005

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, 3/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, 3/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-322826 A (Sony Corp.), 24 November, 2000 (24.11.00), Par. Nos. [0025], [0050] to [0060]; Figs. 3, 5 (Family: none)	1-20
A	JP 2002-100116 A (Sony Corp.), 05 April, 2002 (05.04.02), Abstract & US 2002/0184537 A1 & US 2002/0157012 A1 & EP 1302944 A1 & EP 1302945 A1 & WO 2002/007161 A1 & WO 2002/007162 A1	1-20
A	JP 7-134548 A (Fujitsu Ltd.), 23 May, 1995 (23.05.95), Abstract; Par. No. [0015] (Family: none)	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 April, 2005 (11.04.05)	10 May, 2005 (10.05.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００５／００３００５

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F12/14, 3/06

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.[7]　G06F12/14, 3/06

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００５年
日本国実用新案登録公報	１９９６－２００５年
日本国登録実用新案公報	１９９４－２００５年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000-322826 A （ソニー株式会社） 2000.11.24, 段落【００２５】、【００５０】－【００６０】、図３、図５（ファミリーなし）	１－２０
A	JP 2002-100116 A （ソニー株式会社） 2002.04.05, 【要約】 & US 2002/0184537 A1 & US 2002/0157012 A1 & EP 1302944 A1 & EP 1302945 A1 & WO 2002/007161 A1 & WO 2002/007162 A1	１－２０
A	JP 7-134548 A （富士通株式会社） 1995.05.23, 【要約】、段落【００１５】 （ファミリーなし）	１－２０

☐ Ｃ欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １１．０４．２００５	国際調査報告の発送日　10.05.2005
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　5N　9071 平井　誠 電話番号　０３－３５８１－１１０１　内線　３５８６

様式ＰＣＴ／ＩＳＡ／２１０（第2ページ）（２００４年1月）