(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5574858号
(P5574858)
(45)発行日　平成26年8月20日(2014.8.20)　(24)登録日　平成26年7月11日(2014.7.11)

(51)Int.Cl.　　F I
G06F 21/60 (2013.01)　　G06F 21/24 160B
G06F 21/62 (2013.01)　　G06F 21/24 166A
G06F 3/06 (2006.01)　　G06F 3/06 304H

請求項の数 5　(全 11 頁)

(21)出願番号　特願2010-154563 (P2010-154563)
(22)出願日　平成22年7月7日 (2010.7.7)
(65)公開番号　特開2012-18501 (P2012-18501A)
(43)公開日　平成24年1月26日 (2012.1.26)
審査請求日　平成25年7月3日 (2013.7.3)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100145827
弁理士　水垣　親房
(72)発明者　三上　文夫
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理装置の制御方法、プログラム

(57)【特許請求の範囲】
【請求項１】
ジョブの実行に用いるデータを記憶する第１の記憶手段と、
ジョブの実行に用いるデータを記憶するソリッドステートドライブから成る第２の記憶手段と、
ジョブの実行に用いるデータを削除するためのレベルを設定する設定手段と、
前記ジョブで利用する記憶手段が第１の記憶手段であるか、第２の記憶手段であるかを識別する識別手段と、
前記識別手段が第１の記憶手段を利用すると識別し、かつ、前記設定手段により設定されたレベルが所定レベルである場合、前記ジョブのデータを前記第１の記憶手段に格納し、ジョブ実行時に格納されたデータを上書きし、
前記識別手段が第２の記憶手段を利用すると識別し、かつ、前記設定手段により設定されたレベルが所定レベルである場合、ジョブ実行時にジョブのデータを暗号化して前記第２の記憶手段に格納する制御手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
前記制御手段は、前記識別手段が第１の記憶手段を利用すると識別し、かつ、前記設定手段により設定されたレベルが所定レベルよりも低い場合、前記ジョブのデータを前記第１の記憶手段に格納し、ジョブ実行時に格納されたデータを上書きしないように制御し、
前記識別手段が第２の記憶手段を利用すると識別し、かつ、前記設定手段により設定さ

れたレベルが所定レベルよりも低い場合、ジョブ実行時にジョブのデータを暗号化して第２の記憶手段に格納することを実行しないように制御することを特徴とする請求項１記載の情報処理装置。
【請求項３】
前記第１の記憶手段は、ハードディスクドライブであることを請求項１記載の情報処理装置。
【請求項４】
ジョブの実行に用いるデータを記憶する第１の記憶手段と、ジョブの実行に用いるデータを記憶するソリッドステートドライブから成る第２の記憶手段と、を備える情報処理装置の制御方法であって、
ジョブの実行に用いるデータを削除するためのレベルを設定する設定工程と、
前記ジョブで利用する記憶手段が第１の記憶手段であるか、第２の記憶手段であるかを識別する識別工程と、
前記識別工程が第１の記憶手段を利用すると識別し、かつ、前記設定工程により設定されたレベルが所定レベルである場合、前記ジョブのデータを前記第１の記憶手段に格納し、ジョブ実行時に格納されたデータを上書きし、
前記識別工程が前記第２の記憶手段を利用すると識別し、かつ、前記設定工程により設定されたレベルが所定レベルである場合、ジョブ実行時にジョブのデータを暗号化して前記第２の記憶手段に格納する制御工程と、
を備えることを特徴とする情報処理装置の制御方法。
【請求項５】
請求項４に記載の情報処理装置の制御方法をコンピュータに実行させることを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、情報処理装置の制御方法、及びプログラムに関するものである。
【背景技術】
【０００２】
従来、情報処理装置において、データの漏洩に係るセキュリティレベルを高く設定した場合に、不揮発性記憶装置、例えばハードディスク（ＨＤＤ）のデータを使用後に完全消去することがあった。下記特許文献１には、ＨＤＤのデータを他のデータで上書きすることにより、ＨＤＤのデータを使用後に完全消去する技術が記載されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００４－００５５８６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、半導体記憶装置、例えばSolid State Drive（ＳＳＤ）のデータ消去方法として、ＨＤＤと同様の方式（消去したいＬＢＡにデータを上書きする方式）を採用したとしても、ＳＳＤ内のデータを完全消去することはできない。ここで、ＬＢＡとは、ハードディスク内のすべてのセクタに通し番号を振り、その通し番号によってセクタを指定する方式である。
【０００５】
しかし、ＳＳＤに対するデータ消去処理として、ＨＤＤと同様の方式を採用して同じＬＢＡに別データを上書きしても、ウエアレベリング動作によって他の物理アドレスがそのＬＢＡに割り当てられて書き込まれることになり、ＳＳＤ内のどこかにデータが残留する

ことになってしまうからである。
【０００６】
ここで、ウエアレベリング動作とは、分散書き込みを行ってフラッシュメモリの寿命を延ばす手法の１つである。より具体的には、ウエアレベリングを行う半導体記憶装置は、書き込み回数の少ないブロックをなるべく使用するようにブロックを置き換えて書き込みを行っていく。
【０００７】
そのため、このような半導体記憶装置に対してＨＤＤと同様のデータ消去方法を適用してもウエアレベリングのブロック置換え制御によって、見かけ上同じＬＢＡに別データを上書きしても、実際には他の物理アドレスを指定している。このたため、ＳＳＤ上では置換え前のブロックに情報が残っている可能性も考えられる。
【０００８】
このため、ジョブ実行終了時にデータを消去するために、データ消去時のセキュリティレベル（安全性レベル）を高く設定した場合に、ＳＳＤ内のチップ内にはどこかに消去すべきであったデータが残存する可能性がある。
【０００９】
これにより、ユーザが設定する安全性のレベルが高く設定された場合であっても、実際には、ＳＳＤ上に消去すべきデータが残存し、データの機密性の要求を満たすことができない場合があるという課題があった。
【００１０】
本発明は、上記の課題を解決するためになされたもので、本発明の目的は、設定されるセキュリティレベルに応じて、接続される記憶装置の属性に適応したデータ消去処理を行える仕組みを提供することである。
【課題を解決するための手段】
【００１１】
上記目的を達成する本発明の情報処理装置は以下に示す構成を備える。
ジョブの実行に用いるデータを記憶する第１の記憶手段と、ジョブの実行に用いるデータを記憶するソリッドステートドライブから成る第２の記憶手段と、ジョブの実行に用いるデータを削除するためのレベルを設定する設定手段と、前記ジョブで利用する記憶手段が第１の記憶手段であるか、第２の記憶手段であるかを識別する識別手段と、前記識別手段が第１の記憶手段を利用すると識別し、かつ、前記設定手段により設定されたレベルが所定レベルである場合、前記ジョブのデータを前記第１の記憶手段に格納し、ジョブ実行時に格納されたデータを上書きし、前記識別手段が第２の記憶手段を利用すると識別し、かつ、前記設定手段により設定されたレベルが所定レベルである場合、ジョブ実行時にジョブのデータを暗号化して前記第２の記憶手段に格納する制御手段と、を備えることを特徴とする。
【発明の効果】
【００１２】
本発明によれば、設定されるセキュリティレベルに応じて、接続される記憶装置の属性に適応したデータ消去処理を行える。
【図面の簡単な説明】
【００１３】
【図１】情報処理装置の構成を説明するブロック図である。
【図２】情報処理装置のデータ処理手順を示すフローチャートである。
【図３】情報処理装置の構成を説明するブロック図である。
【図４】情報処理装置のデータ処理手順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】
【００１４】
次に本発明を実施するための最良の形態について図面を参照して説明する。
〔第１実施形態〕

以下、本発明を実施するための最良の形態について図を用いて説明する。
図１は、本実施形態を示す情報処理装置の構成を説明するブロック図である。本例は、記憶装置としてディスクを回転駆動して情報を記憶するＨＤＤと、半導体記憶装置としてＳＳＤを備える情報処理装置の例を示す。また、本実施形態として、情報処理装置の例としてＭＦＰ（Multi Function Peripheral）の例を示すが、これに限定されるものではない。本例は、後述する１つのハードディスクコントローラで、ＨＤＤとＳＳＤのいずれか一方へのアクセスを制御する例である。なお、本実施形態では、第１の記憶手段をハードディスクドライブで構成し、第２の記憶手段をソリッドステートドライブで構成する例である。
【００１５】
図１において、２００はシステム制御部であり、ＭＦＰのコントローラ機能を有するものである。システム制御部２００は、操作部４０１、スキャナ部４０２、プリンタ部４０３と電気的に接続されており、一方ではＬＡＮを介してＰＣや外部の装置などと画像データやデバイス情報の通信が可能となっている。
【００１６】
システム制御部２００において、ＣＰＵ２０１は、ＲＯＭ２５３に記憶された制御プログラム等に基づいてシステムバスに接続されたデバイスのアクセスを統括的に制御する。
ＤＲＡＭ２５２は、ＣＰＵ２０１が動作するためのシステムワークメモリであり、暗号化モジュールの暗号鍵を一時記憶するためのメモリでもあり、電源オフにより記憶した内容が消去される。ＳＲＡＭ２５４は、記憶した内容を電源オフ後も保持しておくよう電池によるバックアップがされている。ＲＯＭ２５３には装置のブートプログラムが格納されている。
【００１７】
２０２はハードディスクコントローラであり、ＳＡＴＡインタフェースで接続された暗号化モジュール２６０を介してＳＳＤ２６２あるいはハードディスク２６３とＳＡＴＡインタフェースにより接続される。
【００１８】
本実施形態ではＳＳＤかハードディスクのどちらか一方が接続されるがまずＳＳＤが接続されているものとする。
操作部Ｉ／Ｆ２０５は、システムバス２０３と操作部４０１とを接続するためのインタフェース部である。この操作部Ｉ／Ｆ２０５は、操作部４０１に表示するための画像データをシステムバス２０３から受け取り操作部４０１に出力すると共に、操作部４０１から入力された情報をシステムバス２０３へと出力する。
【００１９】
Ｎｅｔｗｏｒｋ　Ｉ／Ｆ２０６はＬＡＮ及びシステムバス２０３に接続される。画像バス２２０は画像データをやり取りするための伝送路であり、ＰＣＩバスで構成されている。
【００２０】
なお、操作部４０１は、所定のジョブを実行する際に使用されるＳＳＤまたはＨＤＤに対して実行すべきデータ消去レベルを、高い又は低いの２段階で設定する。また、設定可能消去レベルをさらに増やしたり、実行するジョブ種別に割り当てられた消去レベルテーブルとして管理して、実行するジョブ種別で消去レベルを確定するように制御してもよい。
【００２１】
スキャナ画像処理部２１２は、スキャナ部４０２からスキャナＩ／Ｆ２１１を介して受け取った画像データに対して、補正、加工、及び編集を行う。なお、スキャナ画像処理部２１２は、受け取った画像データがカラー原稿であるか白黒原稿であるか、文字原稿であるか写真原稿であるかなどを判定する。そして、その判定結果を画像データに付随させる。こうした付随情報を像域データと称する。圧縮部２１３は画像データを受け取り、この画像データを３２画素×３２画素のブロック単位に分割する。

【００２２】
＜コピー動作の説明＞
スキャナ部４０２で読み取られた画像データは、スキャナＩ／Ｆ２１１を介してスキャナ画像処理部２１２に送られる。
【００２３】
圧縮部２１３は、スキャナ画像処理部２１２から出力される画像データを３２画素×３２画素のブロック単位に分割しタイルデータを生成し圧縮する。ここで圧縮された画像データはＤＲＡＭ２５２に送られ一時的に格納される。なお、この画像データは必要に応じて画像変換部２１７に送られ画像処理が施された上で再びＤＲＡＭ２５２に送られ格納される。
【００２４】
この後、画像データはＤＲＡＭ２５２からハードディスクコントローラ２０２へ転送される。ハードディスクコントローラ２０２にはＳＡＴＡインタフェースを介して暗号化モジュール２６０が接続され、必要に応じて暗号化されたデータはＳＡＴＡインタフェースを介してＳＳＤ２６２に書き込まれる。
【００２５】
次に、ＳＳＤから読み出されたデータは暗号化モジュール２６０で復号化されてシステムバス２０３へ送出される。
その後、画像データはシステムバス２０３から伸張部２１６に送られる。伸張部２１６は、この画像データを伸張する。さらに伸張部２１６は、伸張後の複数のタイルデータからなる画像データをラスタ展開する。ラスタ展開後の画像データはプリンタ画像処理部２１５に送られる。プリンタ画像処理部２１５において処理された画像データはプリンタＩ／Ｆ２１４を介してプリンタ部４０３に送られる。
【００２６】
画像データをＳＳＤ２６２あるいはハードディスク２６３を経由させるのは、ページ入れ換え処理等を実施するための作業領域を確保するためである。
本実施形態では画像データの記憶される媒体としてＳＳＤ２６２かハードディスク（ＨＤＤ）２６３のいずれかが接続可能な構成のものである。
＜制御フローの説明＞
図２は、本実施形態を示す情報処理装置のデータ処理手順を示すフローチャートである。本例は、ＣＰＵ２０１により、ＨＤＤ２６３またはＳＳＤ２６２に記憶された情報を消去する処理例である。各ステップは、ＣＰＵ２０１がＲＯＭ２５３に記憶された制御プログラムをＤＲＡＭ２５２にロードして実行することで実現される。以下、実行するジョブで利用する記憶装置を識別して、かつ、設定された消去レベルに従いジョブ終了毎にＨＤＤまたはＳＳＤに適応したデータ消去する処理について詳述する。
【００２７】
Ｓ１で、ジョブ投入されたことを確認したら、Ｓ２で、ＣＰＵ２０１は、ジョブ消去モードがあらかじめユーザによって操作部４０１から設定されているか否かを判定する。ここで、ジョブ消去モードが設定されているとＣＰＵ２０１が判断した場合、Ｓ２０へ進み、ジョブ消去モードが設定されていないと判断した場合、本処理を終了する。
次に、Ｓ２０で、ＣＰＵ２０１は、システムに接続されている記憶装置がＳＳＤ２６２かＨＤＤ２６３であるのかを識別する。ここで、ＳＳＤ２６２が接続されているとＣＰＵ２０１が識別した場合、Ｓ３へ進み、ＨＤＤ２６３が接続されているとＣＰＵ２０１が識別した場合は、Ｓ２１へ進む。
【００２８】
Ｓ３では、ＣＰＵ２０１は、あらかじめユーザによって操作部４０１から設定されてＳＲＡＭ２５４等に記憶されているジョブ消去の安全性レベルの指定値を調べる。なお、ＳＲＡＭ２５４に代えて、図示しないＮＶＲＡＭであってもよい。
【００２９】
ここで、ジョブ消去の安全性レベルの指定値が高いと指定されているとＣＰＵ２０１が

判定した場合は、Ｓ４へ進む。そして、Ｓ４で、ＣＰＵ２０１は図１に示した暗号化モジュール２６０へ設定するための暗号鍵を生成する。

【００３０】

ここで、ＣＰＵ２０１は、暗号鍵をＤＲＡＭ２５２上に生成するため電源保持期間中のみ暗号鍵が維持される。

次に、Ｓ５で、ＣＰＵ２０１は、生成された鍵を暗号化モジュール２６０へ設定し、Ｓ６で、ＣＰＵ２０１は、暗号化モジュール２６０に対して暗号化動作をイネーブルに設定する。

【００３１】

次に、Ｓ７で、ＣＰＵ２０１は、ジョブを実行して、処理対象の画像データをハードディスクコントローラ２０２を介して暗号化モジュール２６０で暗号化して、ＳＳＤ２６２へのリードライトが実行される。ここで、ジョブとは、ＭＦＰの機能処理であって、図示しないＵＩ画面で指定されたジョブ、あるいは受信したプリントジョブ等が含まれる。

【００３２】

次に、Ｓ８で、ＣＰＵ２０１は、指定されたジョブが終了しているかどうかを判定する。ここで、ジョブを終了しているとＣＰＵ２０１が判定した場合、Ｓ９で、ＣＰＵ２０１は、ＤＲＡＭ２５２上に保持させている暗号鍵を消去し、同時に暗号化モジュール２６０の暗号鍵も消去して、本処理を終了する。

【００３３】

これによりジョブが終了した後に、ＳＳＤ２６２上に残留している画像データは復号化できなくなっているため、ＳＳＤ２６２上にジョブの履歴が残留せず機密性を維持することができる。

【００３４】

一方、Ｓ３で、ジョブ消去の安全性レベルの指定値が低いとＣＰＵ２０１が判定した場合は、Ｓ１０へ進む。そして、Ｓ１０で、暗号化モジュール２６０をディスエイブルに設定して、Ｓ１１で、ＣＰＵ２０１がジョブが終了したと判断した場合、本処理を終了する。

【００３５】

一方、Ｓ２０で、接続されている記憶装置がＨＤＤであると判定されたときはＳ２１へ進む。そして、Ｓ２１で、暗号化モジュール２６０をディスエイブルに設定する。

次に、Ｓ２２で、ＣＰＵ２０１は、あらかじめユーザによって操作部４０１から設定されているジョブ消去の安全性レベルの指定値が高いか低いかを判定する。ここで、ＣＰＵ２０１は、ユーが操作部４０１を用いて設定した後、ＳＲＡＭ２５４に保持されたジョブ消去の安全性レベルに対応する設定値を参照することで、ジョブ消去の安全性レベルの指定値が高いか低いかを判定する。

ここで、ジョブ消去の安全性レベルの指定値が高いレベルが指定されているとＣＰＵ２０１が判定した場合、Ｓ２３へ進む。

そして、Ｓ２３で、ジョブ実行時は平文でＨＤＤ２６３へアクセスし、Ｓ２４で、ジョブが終了したとＣＰＵ２０１が判断した場合は、Ｓ２５で、ＣＰＵ２０１は、ジョブ実行に伴うＨＤＤ２６３の使用した領域にランダムデータ（特定データ）を１回あるいは複数回書き込んで、本処理を終了する。

【００３６】

一方、Ｓ２２で、ジョブ消去の安全性レベルの指定値が低いとＣＰＵ２０１が判断した場合は、ＣＰＵ２０１は、ジョブ終了時にはジョブ実行に伴いＨＤＤ２６３で使用した画像データを残留したまま、何も消去処理を実行することなく、本処理を終了する。

【００３７】

なお、Ｓ４で、ＣＰＵ２０１が生成する暗号鍵はコントローラ内部で、ジョブ毎にランダムに生成されるものであり、外部から類推することのできないものである。

また、本実施形態では、ＳＳＤが接続されている場合、暗号化されたデータがＳＳＤ上に残留するが、ＳＳＤの構成上、完全消去はできないため外部から復元できないようにす

るために暗号鍵をジョブ毎に消去する構成としている。

【００３８】

一方、ＨＤＤが接続されている場合は、同一アドレスへ複数回ランダムデータを書き込むことでデータの痕跡をかく乱することができるため暗号化する必要がない。

また、暗号化モジュールの構成が暗号化と複合化処理に所定の時間が必要となる場合、ハードディスクが接続される場合は暗号化を用いないとすることで装置としての処理速度に影響を与えないようにすることができる。

【００３９】

〔第２実施形態〕

図３は、本実施形態を示す情報処理装置の構成を説明するブロック図である。本例は、記憶装置としてディスクを回転駆動して情報を記憶するＨＤＤと、半導体記憶装置としてＳＳＤを備える情報処理装置の例を示す。また、本実施形態として、情報処理装置の例としてＭＦＰ（Multi Function Peripheral）の例を示すが、これに限定されるものではない。本例は、後述する２つのハードディスクコントローラで、それぞれ独立してＨＤＤまたはＳＳＤのアクセスを制御する例である。

【００４０】

図３において、システムバス２０３に第一のハードディスクコントローラ２０２が接続され、暗号化モジュール２６０を介してＳＳＤ２６２へ接続されている。またシステムバス２０３には第二のハードディスクコントローラ２０４が接続され、ＨＤＤ２６３へ接続されている。

【００４１】

ＳＳＤ２６２は、例えば８０ＧＢの小容量のデータを保持するものであり、標準の製品出荷形態として搭載されている。

ＨＤＤ２６３は、例えば大容量１０００ＧＢであり、オプションとして接続されるものである。小容量ハードディスクはシステムプログラムと、一時的にデータを記憶する媒体として使用され、大容量ハードディスクはユーザデータを保管するという使用方法が想定されている。

【００４２】

ＳＳＤはコストが割高のため、小容量の記憶媒体としては信頼性確保のため適するが、大容量の記憶媒体としてはＨＤＤに実用性があり、本実施形態では両記憶媒体を搭載する形態である。

【００４３】

本実施形態ではＳＳＤを標準で搭載している装置において、オプションとして大容量のＨＤＤを搭載している装置を例にして説明する。

ＣＰＵ２０１は、システムの起動時にはＳＳＤ２６２からプログラムをロードする。また、ジョブ実行時に一時的に画像データを記憶する場所として使用する際にはＳＳＤ２６２を使用する。

【００４４】

近年の複合機には、ビッグボックス等と呼ばれるユーザデータを保存する機能が搭載されており、この機能の実現のためには、ＳＳＤ２６２の小容量、例えば８０ＧＢでは不足しており、大容量の、例えば１０００ＧＢのＨＤＤ２６３のユーザ領域を使用する。

【００４５】

ここで、操作部４０１とからのシステム設定において、ジョブ消去モードが設定されている場合には、ジョブを実行する際には、ＳＳＤ２６２を使用し、暗号化モジュール２６０で暗号化復号化したデータによってＳＳＤ２６２へアクセスする。

【００４６】

また、ジョブ終了時にはこのジョブで用いた暗号鍵を廃棄することでＳＳＤ２６２へ書き込まれたデータは無効化される。

一方、ビッグボックスへのデータ書込み指示に対してはＨＤＤ２６３に書き込みを行う。

ユーザからのＨＤＤ２６３のビッグボックス上のファイル消去指示がなされた場合には、ＨＤＤ２６３上のデータを消去することとなり、ＣＰＵ２０１は、消去領域に対してランダムデータの複数回書込みを行う。

【００４７】

図４は、本実施形態を示す情報処理装置のデータ処理手順を示すフローチャートである。本例は、ＣＰＵ２０１により、ＨＤＤ２６３またはＳＳＤ２６２に記憶された情報を消去する処理例である。各ステップは、ＣＰＵ２０１がＲＯＭ２５３に記憶された制御プログラムをＤＲＡＭ２５２にロードして実行することで実現される。なお、本実施形態では、図２に示した第１実施形態と異なるステップを中心に説明し、同一のステップの説明は省略する。

【００４８】

Ｓ１で、ＣＰＵ２０１がジョブが投入されたことを確認したら、Ｓ３１へ進み、ジョブに用いる記憶装置がＨＤＤであるのか、ＳＳＤであるのかを判断する。ここで、ＣＰＵ２０１は、ジョブの種別、例えばプリントジョブであって、ユーザがログイン情報を用いてボックス領域を使用するようなジョブであれば、ＨＤＤを使用すると判定する。なお、判定は、ジョブで使用するメモリ使用量等に応じて判定してもよく、または、ユーザ情報、グループ情報等に応じて使用する記憶装置の判定を行ってもよい。

【００４９】

ここで、ＣＰＵ２０１がＨＤＤ２６３を使用すると判定した場合、Ｓ３２で、ＣＰＵ２０１は、あらかじめユーザによって操作部４０１から設定されてＳＲＡＭ２５４等に記憶されているジョブ消去の安全性レベルの指定値を調べる。なお、ＳＲＡＭ２５４に代えて、図示しないＮＶＲＡＭであってもよい。

【００５０】

ここで、ジョブ消去の安全性レベルの指定値が高いと指定されているとＣＰＵ２０１が判定した場合は、Ｓ２３へ進み、第１実施形態と同様にデータ処理を行う。

一方、Ｓ３２で、ジョブ消去の安全性レベルの指定値が低いと指定されているとＣＰＵ２０１が判定した場合は、Ｓ３３へ進む。

そして、Ｓ３３で、ジョブ実行時は平文でＨＤＤ２６３へアクセスし、Ｓ３４で、ジョブが終了したとＣＰＵ２０１が判断した場合は、データ消去処理を実行することなく、本処理を終了する。

【００５１】

本実施形態によれば、セキュリティレベルを高く設定した場合に、記憶装置の種類に応じた適切な方法でデータを消去することができ、記憶装置に記憶されたデータに対して機密性を担保することが可能となる。

【００５２】

より具体的には、例えば以下のような効果が挙げられる。

完全消去することができないＳＳＤに対して、完全消去と同等の効果が得られる。

また、従来例ではジョブ動作が終了してから、消去するまでの間に記憶装置を取り外されてしまえば機密性が危険にさらされていたが、本発明では記憶装置が取り外されても暗号化データが記録されているため漏洩の危険は回避できる。

【００５３】

さらに、従来は上書きによるデータ消去動作をジョブとは別時間で実行していたため、記憶装置とのインタフェース上を流れるデータ量が増大しジョブの処理速度低下を招く場合があった。

【００５４】

しかし、暗号化複合化をリアルタイム処理できる手段を有する装置においては、本発明によりこれを回避できる。

さらに、暗号鍵の消去はＤＲＡＭ等に高々数十ビット存在するだけなので、消去時間は事実上見えてこない。

また、暗号化書込みをハードディスクへの応用すれば、従来の「一括消去」モードを不

要とすることができる。これにより、従来は一括消去動作するまで機密性が危険にさらされていたことを回避できる。

【００５５】

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

【００５６】

本発明は上記実施形態に限定されるものではなく、本発明の趣旨に基づき種々の変形（各実施形態の有機的な組合せを含む）が可能であり、それらを本発明の範囲から除外するものではない。

【００５７】

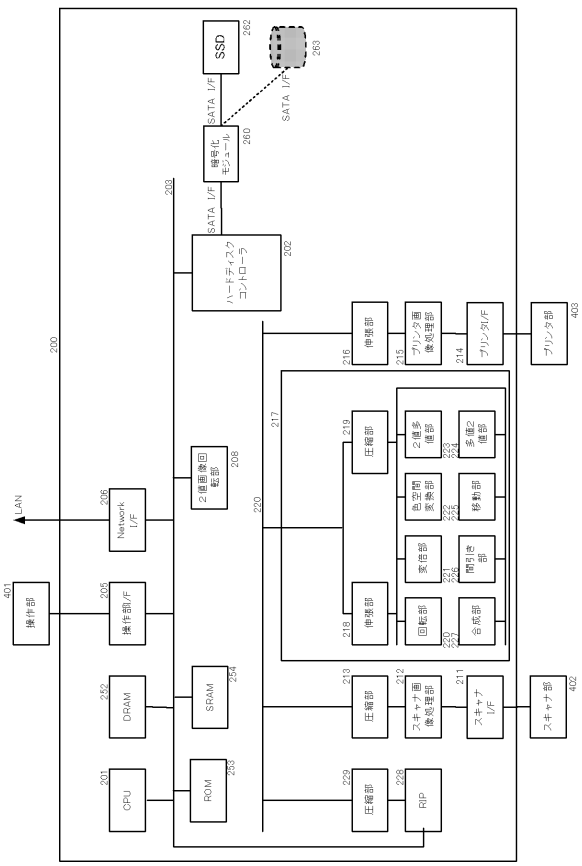
本発明の様々な例と実施形態を示して説明したが、当業者であれば、本発明の趣旨と範囲は、本明細書内の特定の説明に限定されるのではない。

【符号の説明】

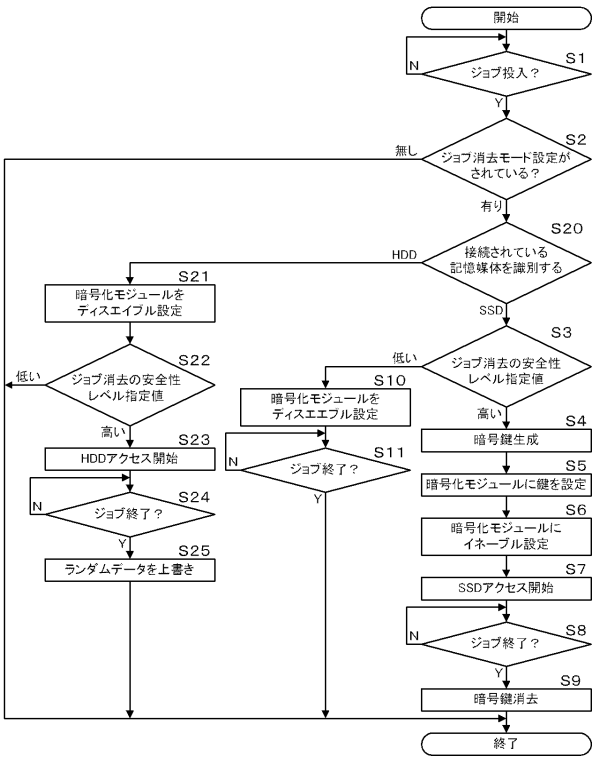
【００５８】

２０２　ハードディスクコントローラ
２６０　暗号化モジュール
２６２　ＳＳＤ
２６３　ＨＤＤ

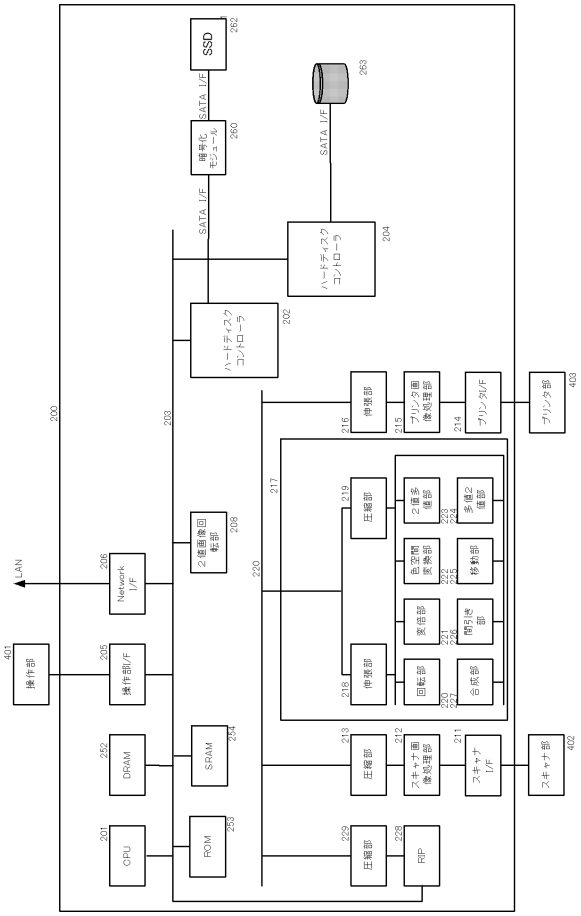
【図１】



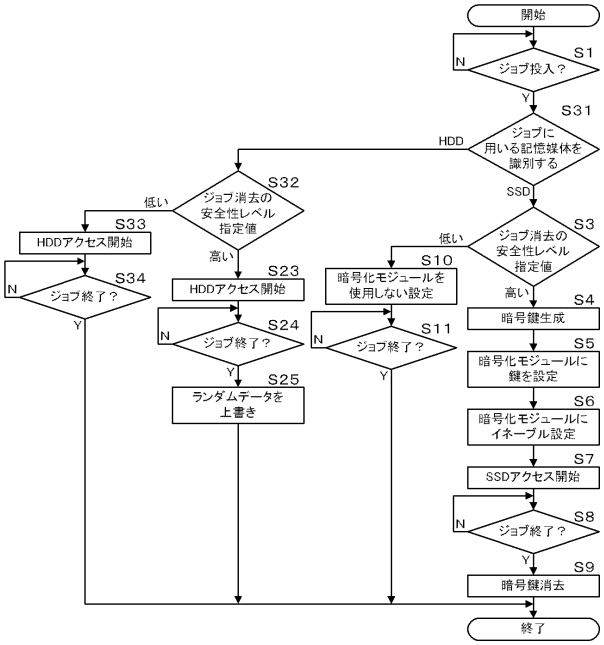
【図２】



【図３】


SSD
262
SATA I/F
260
SATA I/F
263
SATA I/F
ハードディスク
コントローラ
204
ハードディスク
コントローラ
202
200
203
LAN
206
Network
I/F
208
2値画像回
転部
220
401
操作部
205
操作部I/F
252
DRAM
254
SRAM
201
CPU
253
ROM
伸張部
216
プリンタ画
像処理部
215
プリンタI/F
214
プリンタ部
403
217
圧縮部
219
2値多
値部
223
多値2
値部
224
回転変倍
部
222
移動部
221
変倍部
225
間引き
部
伸張部
218
回転部
220
合成部
227
圧縮部
213
スキャナ画
像処理部
212
スキャナ
I/F
211
スキャナ部
402
圧縮部
229
RIP
228

【図４】


開始
S1
ジョブ投入？
N
Y
S31
ジョブに
用いる記憶媒体を
識別する
HDD
SSD
S32
ジョブ消去の
安全性レベル
指定値
低い
高い
S33
HDDアクセス開始
S34
ジョブ終了？
N
Y
S23
HDDアクセス開始
S24
ジョブ終了？
N
Y
S25
ランダムデータを
上書き
S3
ジョブ消去の
安全性レベル
指定値
低い
高い
S10
暗号化モジュールを
使用しない設定
S11
ジョブ終了？
N
Y
S4
暗号鍵生成
S5
暗号化モジュールに
鍵を設定
S6
暗号化モジュールに
イネーブル設定
S7
SSDアクセス開始
S8
ジョブ終了？
N
Y
S9
暗号鍵消去
終了

フロントページの続き

(56)参考文献 特開２０１０－１２４０７６（ＪＰ，Ａ）
特開２００４－００５５８６（ＪＰ，Ａ）
特開２０１０－２８８１２３（ＪＰ，Ａ）
特開２００６－２７６９０８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１