(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2005-275812
(P2005-275812A)
(43)公開日　平成17年10月6日(2005.10.6)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 12/14	G06F	12/14	550A	5B017
	G06F	12/14	530B	

審査請求 未請求　請求項の数 18　ＯＬ　（全 17 頁）

(21)出願番号　特願2004-88100(P2004-88100)
(22)出願日　平成16年3月24日(2004.3.24)

(71)出願人　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　100081880
弁理士　渡部　敏彦
(72)発明者　▲高▼田　智行
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
(72)発明者　鈴木　範之
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
(72)発明者　伊藤　博康
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

最終頁に続く

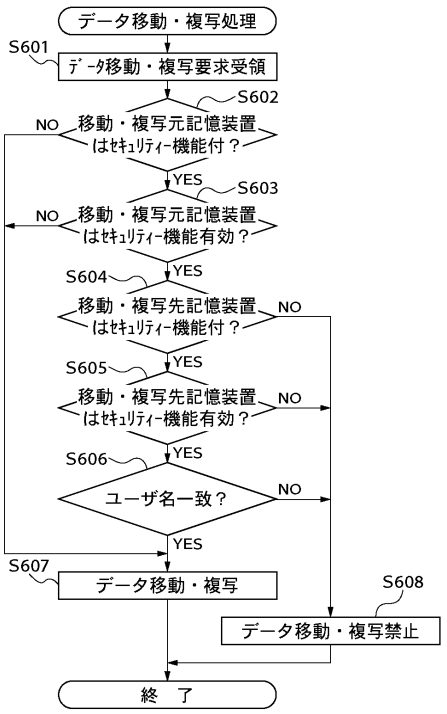
(54)【発明の名称】情報処理装置及びその制御方法、並びに制御プログラム及び記憶媒体

(57)【要約】

【課題】　ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができる情報処理装置及びその制御方法、並びに制御プログラム及び記憶媒体を提供する。

【解決手段】　本体装置１００は、ユーザにより入力装置１１０に入力されたデータの移動・複写要求を受領し、データの移動・複写元記憶装置がセキュリティー機能付記憶装置であり、データの移動・複写元記憶装置のセキュリティー機能が有効に設定されているときは、データの移動・複写先記憶装置がセキュリティー機能付記憶装置でないか、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されていないか、又はデータの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していないときは、出力装置１２０に報知画面を表示し、データの移動・複写を禁止する。

【選択図】　図６



【特許請求の範囲】
【請求項１】
複数の記憶装置を備える情報処理装置において、移動元記憶装置から移動先記憶装置へデータを移動する際に、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報を比較するセキュリティー情報比較手段と、前記セキュリティー情報比較手段による比較結果に基づいて、前記データの移動を制御するデータ移動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】
前記データ移動制御手段は、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときは、前記データの移動を許可しない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】
前記データ移動制御手段は、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときに、前記データの移動を行うか否かの指示を要求する指示要求手段と、前記指示を取得する取得手段とを備え、前記データの移動を行う指示を取得したときは前記データの移動を許可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４】
前記セキュリティー情報はユーザ認証機能の有無を含み、前記セキュリティー情報比較手段は、前記移動元記憶装置は前記ユーザ認証機能を有しているが、前記移動先記憶装置は前記ユーザ認証機能を有していないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
前記セキュリティー情報はユーザ認証機能が有効に設定されているか否かを含み、前記セキュリティー情報比較手段は、前記移動元記憶装置のユーザ認証機能は有効に設定されているが、前記移動先記憶装置のユーザ認証機能は有効に設定されていないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする請求項１乃至４のいずれか１項に記載の情報処理装置。
【請求項６】
前記セキュリティー情報はユーザ識別情報を含み、前記セキュリティー情報比較手段は、前記移動元記憶装置のユーザ識別情報及び前記移動先記憶装置のユーザ識別情報が一致しないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする請求項１乃至５のいずれか１項に記載の情報処理装置。
【請求項７】
前記セキュリティー情報比較手段による比較結果を表示する表示手段を備えることを特徴とする請求項１乃至６のいずれか１項に記載の情報処理装置。
【請求項８】
前記データの移動は、前記データの複写を含むことを特徴とする請求項１乃至７のいずれか１項に記載の情報処理装置。
【請求項９】
複数の記憶装置を備える情報処理装置の制御方法において、移動元記憶装置から移動先記憶装置へデータを移動する際に、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報を比較するセキュリティー情報比較ステップと、前記セキュリティー情報比較ステップにおける比較結果に基づいて、前記データの移動を制御するデータ移動制御ステップ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１０】
前記データ移動制御ステップは、前記移動元記憶装置のセキュリティー情報及び前記移

動先記憶装置のセキュリティー情報が一致しないときは、前記データの移動を許可しないことを特徴とする請求項９記載の情報処理装置の制御方法。
【請求項１１】
前記データ移動制御ステップは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときに、前記データの移動を行うか否かの指示を要求する指示要求ステップと、前記指示を取得する取得ステップとを備え、前記データの移動を行う指示を取得したときは前記データの移動を許可することを特徴とする請求項９記載の情報処理装置の制御方法。
【請求項１２】
前記セキュリティー情報はユーザ認証機能の有無を含み、前記セキュリティー情報比較ステップは、前記移動元記憶装置は前記ユーザ認証機能を有しているが、前記移動先記憶装置は前記ユーザ認証機能を有していないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする請求項９乃至１１のいずれか１項に記載の情報処理装置の制御方法。
【請求項１３】
前記セキュリティー情報はユーザ認証機能が有効に設定されているか否かを含み、前記セキュリティー情報比較ステップは、前記移動元記憶装置のユーザ認証機能は有効に設定されているが、前記移動先記憶装置のユーザ認証機能は有効に設定されていないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする請求項９乃至１２のいずれか１項に記載の情報処理装置の制御方法。
【請求項１４】
前記セキュリティー情報はユーザ識別情報を含み、前記セキュリティー情報比較ステップは、前記移動元記憶装置のユーザ識別情報及び前記移動先記憶装置のユーザ識別情報が一致しないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする請求項９乃至１３のいずれか１項に記載の情報処理装置の制御方法。
【請求項１５】
前記セキュリティー情報比較ステップにおける比較結果を表示する表示ステップを備えることを特徴とする請求項９乃至１４のいずれか１項に記載の情報処理装置の制御方法。
【請求項１６】
前記データの移動は、前記データの複写を含むことを特徴とする請求項９乃至１５のいずれか１項に記載の情報処理装置の制御方法。
【請求項１７】
複数の記憶装置を備える情報処理装置の制御プログラムにおいて、移動元記憶装置から移動先記憶装置へデータを移動する際に、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報を比較するセキュリティー情報比較モジュールと、前記セキュリティー情報比較モジュールによる比較結果に基づいて、前記データの移動を制御するデータ移動制御モジュールとをコンピュータに実行させることを特徴とする情報処理装置の制御プログラム。
【請求項１８】
請求項１７記載のプログラムを格納することを特徴とするコンピュータ読取り可能な記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置及びその制御方法、並びに制御プログラム及び記憶媒体に関し、特に、複数の記憶装置を具備する情報処理装置及びその制御方法、並びに制御プログラム及び記憶媒体に関する。
【背景技術】

【０００２】
近年、ハードディスク等の記憶装置の大容量化が進んでおり、マイクロドライブ、ｉＶＤＲ（ｉＶＤＲコンソーシアムホームページhttp://www.ivdr.org/index_j.html参照）等、小型且つ大容量の可搬型記憶装置の製品化、又は製品化へ向けた検討がなされている。これらの記憶装置の多くは、ＡＴＡ／ＡＴＡＰＩ、ＳＣＳＩ、ＰＣＭＣＩＡ、ＵＳＢ、ＩＥＥＥ１３９４等の汎用インターフェース規格を用いており、その規格をサポートする多くの機器で共通に利用することができる。そのため、上記記憶装置は広く普及しているが、一方で、汎用インターフェース規格を用いているので、第三者が記憶装置内に記憶されたデータにアクセスすることも簡単であり、ユーザの意図しない第三者に記憶装置内に記憶されたデータが漏洩する問題があった。

【０００３】
そこで、例えば、ＡＴＡ／ＡＴＡＰＩ規格セキュリティー・モード・フィーチャー・セットにて規定されているパスワードによるアクセス制限機能を実装したハードディスク、及びそれを搭載したパーソナルコンピュータが製品化されている。

【０００４】
また、パスワードによるアクセス制限機能に加え、複数のユーザを登録し、ユーザ毎に書き込み又は読み出し動作を制限する機能を付加した記憶装置が提案されている（例えば、特許文献１参照）。

【特許文献１】特開平１１－２９６４３６号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】
しかしながら、上記記憶装置は、ユーザの意図しない第三者が記憶装置内に記憶されたデータに不正にアクセスすることを防止するが、正規のユーザはデータへのアクセスが可能であり、一旦、アクセスが可能となった後は、自由にデータの移動・複写を行うことができる。

【０００６】
したがって、例えば、ユーザはデータに対するセキュリティーレベルが低下することを意識せずに、ユーザ認証機能の付加された記憶装置等のセキュリティーレベルの高い記憶装置に記憶された秘匿性の高いデータを、セキュリティー機能を持たない記憶装置に移動・複写してしまうことがあり得る。その結果、秘匿性の高いデータがユーザの意図しない第三者に漏洩する危険がある。

【０００７】
大容量可搬型記憶装置がさらに普及し、頻繁にデータの保管及び機器間の移動のために使用されるようになると、ユーザは記憶装置の管理が困難になり、不注意にデータを移動・複写することによるデータ漏洩の危険性が増大する。

【０００８】
本発明の目的は、ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができる情報処理装置及びその制御方法、並びに制御プログラム及び記憶媒体を提供することにある。

【課題を解決するための手段】

【０００９】
上述の目的を達成するために、請求項１記載の情報処理装置は、複数の記憶装置を備える情報処理装置において、移動元記憶装置から移動先記憶装置へデータを移動する際に、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報を比較するセキュリティー情報比較手段と、前記セキュリティー情報比較手段による比較結果に基づいて、前記データの移動を制御するデータ移動制御手段とを備えることを特徴とする。

【００１０】
請求項２記載の情報処理装置は、請求項１記載の情報処理装置において、前記データ移

動制御手段は、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときは、前記データの移動を許可しないことを特徴とする。

【００１１】

請求項３記載の情報処理装置は、請求項１記載の情報処理装置において、前記データ移動制御手段は、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときに、前記データの移動を行うか否かの指示を要求する指示要求手段と、前記指示を取得する取得手段とを備え、前記データの移動を行う指示を取得したときは前記データの移動を許可することを特徴とする。

【００１２】

請求項４記載の情報処理装置は、請求項１乃至３のいずれか１項に記載の情報処理装置において、前記セキュリティー情報はユーザ認証機能の有無を含み、前記セキュリティー情報比較手段は、前記移動元記憶装置は前記ユーザ認証機能を有しているが、前記移動先記憶装置は前記ユーザ認証機能を有していないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする。

【００１３】

請求項５記載の情報処理装置は、請求項１乃至４のいずれか１項に記載の情報処理装置において、前記セキュリティー情報はユーザ認証機能が有効に設定されているか否かを含み、前記セキュリティー情報比較手段は、前記移動元記憶装置のユーザ認証機能は有効に設定されているが、前記移動先記憶装置のユーザ認証機能は有効に設定されていないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする。

【００１４】

請求項６記載の情報処理装置は、請求項１乃至５のいずれか１項に記載の情報処理装置において、前記セキュリティー情報はユーザ識別情報を含み、前記セキュリティー情報比較手段は、前記移動元記憶装置のユーザ識別情報及び前記移動先記憶装置のユーザ識別情報が一致しないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする。

【００１５】

請求項７記載の情報処理装置は、請求項１乃至６のいずれか１項に記載の情報処理装置において、前記セキュリティー情報比較手段による比較結果を表示する表示手段を備えることを特徴とする。

【００１６】

請求項８記載の情報処理装置は、請求項１乃至７のいずれか１項に記載の情報処理装置において、前記データの移動は、前記データの複写を含むことを特徴とする。

【００１７】

請求項９記載の情報処理装置の制御方法は、複数の記憶装置を備える情報処理装置の制御方法において、移動元記憶装置から移動先記憶装置へデータを移動する際に、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報を比較するセキュリティー情報比較ステップと、前記セキュリティー情報比較ステップにおける比較結果に基づいて、前記データの移動を制御するデータ移動制御ステップとを備えることを特徴とする。

【００１８】

請求項１０記載の制御方法は、請求項９記載の制御方法において、前記データ移動制御ステップは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときは、前記データの移動を許可しないことを特徴とする。

【００１９】

請求項１１記載の制御方法は、請求項９記載の制御方法において、前記データ移動制御ステップは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報が一致しないときに、前記データの移動を行うか否かの指示を要求する指示

要求ステップと、前記指示を取得する取得ステップとを備え、前記データの移動を行う指示を取得したときは前記データの移動を許可することを特徴とする。

【００２０】

請求項１２記載の制御方法は、請求項９乃至１１のいずれか１項に記載の制御方法において、前記セキュリティー情報はユーザ認証機能の有無を含み、前記セキュリティー情報比較ステップは、前記移動元記憶装置は前記ユーザ認証機能を有しているが、前記移動先記憶装置は前記ユーザ認証機能を有していないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする。

【００２１】

請求項１３記載の制御方法は、請求項９乃至１２のいずれか１項に記載の制御方法において、前記セキュリティー情報はユーザ認証機能が有効に設定されているか否かを含み、前記セキュリティー情報比較ステップは、前記移動元記憶装置のユーザ認証機能は有効に設定されているが、前記移動先記憶装置のユーザ認証機能は有効に設定されていないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする。

【００２２】

請求項１４記載の制御方法は、請求項９乃至１３のいずれか１項に記載の制御方法において、前記セキュリティー情報はユーザ識別情報を含み、前記セキュリティー情報比較ステップは、前記移動元記憶装置のユーザ識別情報及び前記移動先記憶装置のユーザ識別情報が一致しないときは、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報は一致しないと判定することを特徴とする。

【００２３】

請求項１５記載の制御方法は、請求項９乃至１４のいずれか１項に記載の制御方法において、前記セキュリティー情報比較ステップにおける比較結果を表示する表示ステップを備えることを特徴とする。

【００２４】

請求項１６記載の制御方法は、請求項９乃至１５のいずれか１項に記載の制御方法において、前記データの移動は、前記データの複写を含むことを特徴とする請求項９乃至１５のいずれか１項に記載の情報処理方法。

【００２５】

請求項１７記載の情報処理の制御プログラムは、複数の記憶装置を備える情報処理装置の制御プログラムにおいて、移動元記憶装置から移動先記憶装置へデータを移動する際に、前記移動元記憶装置のセキュリティー情報及び前記移動先記憶装置のセキュリティー情報を比較するセキュリティー情報比較モジュールと、前記セキュリティー情報比較モジュールによる比較結果に基づいて、前記データの移動を制御するデータ移動制御モジュールとをコンピュータに実行させることを特徴とする。

【００２６】

請求項１８記載のコンピュータ読取り可能な記憶媒体は、請求項１７記載のプログラムを格納することを特徴とする。

【発明の効果】

【００２７】

請求項１記載の情報処理装置、請求項９記載の制御方法、請求項１７記載の制御プログラム、及び請求項１８記載の記憶媒体によれば、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報の比較結果に基づいて、データの移動を制御するので、ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができる。

【００２８】

請求項２記載の情報処理装置、請求項１０記載の制御方法によれば、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報が一致しないときは、デー

タの移動を許可しないので、ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができる。

【００２９】

請求項３記載の情報処理装置、請求項１１記載の制御方法によれば、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報が一致しないときに、データの移動を行うか否かの指示を要求し、データの移動を行う指示を取得したときはデータの移動を許可するので、ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができると共に、ユーザの意思を柔軟に反映してデータの移動・複写を行うことができる。

【００３０】

請求項４記載の情報処理装置、請求項１２記載の制御方法によれば、移動元記憶装置はユーザ認証機能を有しているが、移動先記憶装置はユーザ認証機能を有していないときは、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報は一致しないと判定するので、請求項１の効果を確実に奏することができる。

【００３１】

請求項５記載の情報処理装置、請求項１３記載の制御方法によれば、移動元記憶装置のユーザ認証機能は有効に設定されているが、移動先記憶装置のユーザ認証機能は有効に設定されていないときは、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報は一致しないと判定するので、請求項１の効果を確実に奏することができる。

【００３２】

請求項６記載の情報処理装置、請求項１４記載の制御方法によれば、移動元記憶装置のユーザ識別情報及び移動先記憶装置のユーザ識別情報が一致しないときは、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報は一致しないと判定するので、請求項１の効果を確実に奏することができる。

【００３３】

請求項７記載の情報処理装置、請求項１５記載の制御方法によれば、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報の比較結果を表示するので、移動元記憶装置のセキュリティー情報及び移動先記憶装置のセキュリティー情報の比較結果を確認することができる。

【００３４】

請求項８記載の情報処理装置、請求項１６記載の制御方法によれば、データの移動は、データの複写を含むので、ユーザによるデータの記憶装置間での複写動作に対して強固な安全性を確保することができる。

【発明を実施するための最良の形態】

【００３５】

以下、本発明の実施の形態を図面を参照しながら詳述する。

【００３６】

図１は、本発明の実施の形態に係る情報処理装置の構成を概略的に示すブロック図である。

【００３７】

図１において、本発明の実施の形態に係る情報処理装置は、本体装置１００と、入力装置１１０と、出力装置１２０と、複数の記憶装置１３０，１４０，１５０，１６０（以下、「記憶装置１３０～１６０」という）とから成る。

【００３８】

本体装置１００は、ＣＰＵ１０１と、ＲＯＭ１０２と、ＲＡＭ１０３と、入力装置１１０と信号の接続を行う入力装置インターフェース（Ｉ／Ｆ）部１０４と、出力装置１２０と信号の接続を行う出力装置インターフェース（Ｉ／Ｆ）部１０５と、記憶装置１３０～１６０と信号の接続を行う記憶装置インターフェース（Ｉ／Ｆ）部１０６とを備え、入力装置１１０、出力装置１２０、及び記憶装置１３０～１６０の制御を行う。本体装置１０

０は、例えば、パーソナルコンピュータやサーバ等である。
【００３９】
入力装置１１０は、例えば、キーボード、マウス等であり、ユーザにより入力された情報を本体装置１００に送信する。
【００４０】
出力装置１２０は、例えば、ディスプレイ、スピーカ等であり、本体装置１００の命令に基づき、本体装置１００から送信された情報を出力する。
【００４１】
記憶装置１３０～１６０は、磁気記憶媒体（磁気ディスク、磁気テープ等）、光記憶媒体（ＣＤ、ＤＶＤ等）、光磁気記憶媒体（ＭＯディスク等）、又は半導体記憶媒体等の記憶媒体を具備し、データを記憶する装置である。記憶装置１３０～１６０は、記憶装置１３０、１４０のようにコネクタ又はケーブルで本体装置１００に直接接続される固定記憶装置であってもよく、記憶装置１５０、１６０のように夫々アダプタ１７０、１８０を介して本体装置１００に接続され、アダプタから簡単に取り外し可能な可搬型記憶装置であってもよい。
【００４２】
本実施の形態では、記憶装置１３０～１６０はハードディスクドライブ（ＨＤＤ）であるものとして説明する。
【００４３】
図２は、図１における記憶装置１３０の内部構成を概略的に示すブロック図である。
【００４４】
図２において、記憶装置１３０は、本体装置１００との信号の接続をおこなうインターフェース（Ｉ／Ｆ）部１３１と、不揮発性メモリ１３２と、ディスク記憶媒体１３３と、インターフェース部１３１、不揮発性メモリ１３２、及びディスク記憶媒体１３３を制御するディスクコントローラ１３４とを備える。なお、不揮発性メモリ１３２は、ディスクコントローラ１３４内に実装されていてもよい。
【００４５】
記憶装置１４０～１６０の構成も、記憶装置１３０の構成と基本的に同じであり、記憶装置１３０～１６０には、パスワード認証によるアクセス制御等、内部に記憶されたデータに対するセキュリティー機能（ユーザ認証機能）を持ったセキュリティー機能付記憶装置と、セキュリティー機能を持たない記憶装置とが混在している。記憶装置１３０は、セキュリティー機能付記憶装置であるものとして説明する。
【００４６】
図３は、図２の記憶装置１３０が有する記憶領域の構成を示す図である。
【００４７】
図３において、セキュリティー機能付記憶装置１３０は、不揮発性メモリ１３２又はディスク記憶媒体１３３上に、論理的に分割された３つの領域、即ちディスク管理領域３００、ユーザ情報領域３１０、及びデータ領域３２０を有する。
【００４８】
ディスク管理領域３００は、記憶装置がセキュリティー機能付記憶装置であることを示す記憶装置種別情報３０１と、セキュリティー機能が有効であるか否かを示すセキュリティー機能設定情報３０２と、ユーザ情報領域３１０及びデータ領域３２０にアクセスするためのパスワード情報３０３とを記憶している。記憶装置種別情報３０１及びセキュリティー機能設定情報３０２は、本体装置１００より読み出し可能に記憶されているが、パスワード情報３０３は、読み出し不可能に記憶されている。
【００４９】
ユーザ情報領域３１０は、記憶装置ユーザのユーザ名等のユーザ識別情報を記憶する。データ領域３２０は、ユーザによる任意のデータの記憶に使用可能な領域である。
【００５０】
図４は、図２の記憶装置１３０によって実行されるセキュリティー機能解除処理のフロ

ーチャートである。
【００５１】
本処理は、記憶装置１３０の電源投入時に実行される。
【００５２】
図４において、セキュリティー機能付記憶装置１３０のディスクコントローラ１３４は、ディスク管理領域３００からセキュリティー機能設定情報３０２を読み出し（ステップＳ４０１）、セキュリティー機能が有効に設定されているか否かを判別し（ステップＳ４０２）、セキュリティー機能が有効に設定されているときは、本体装置１００からのパスワードの受領を待機する（ステップＳ４０３）。この時点では本体装置１００からのディスク管理領域３００への書き込みコマンドと、ユーザ情報領域３１０及びデータ領域３２０への一切のアクセスコマンドとを破棄し、ディスク管理領域３００への書き込みとユーザ情報領域３１０及びデータ領域３２０への一切のアクセスを許可しない。
【００５３】
パスワードを受領すると（ステップＳ４０３でＹＥＳ）、受領したパスワードとディスク管理領域３００に記憶しているパスワード情報３０３が等しいか否かを判別し（ステップＳ４０４）、受領したパスワードとディスク管理領域３００に記憶しているパスワード情報３０３が等しいときは、セキュリティー機能を解除して、ディスク管理領域３００のセキュリティー機能設定情報３０２にセキュリティー機能を解除したことを示す情報を書き込み（ステップＳ４０５）、本処理を終了する。
【００５４】
ステップＳ４０４の判別の結果、受領したパスワードとディスク管理領域３００に記憶しているパスワード情報３０３が等しくないときは、ステップＳ４０３に戻り、本体装置１００からのパスワードの受領を待機する。
【００５５】
ステップＳ４０２の判別の結果、セキュリティー機能が有効に設定されていないときは、本処理処理を終了する。
【００５６】
本処理において、ステップＳ４０２の判別の結果、セキュリティー機能が有効に設定されていないか、又は、ステップＳ４０５でセキュリティー機能を解除すると、記憶装置１３０は、データ領域３２０へのアクセスコマンドを受領し、データ領域３２０へのアクセスを許可する。さらに、記憶装置１３０は、ディスク管理領域３００のセキュリティー機能設定情報３０２、又はパスワード情報３０３への書き込みコマンドを受領し、セキュリティー機能設定情報３０２、又はパスワード情報３０３の書き換えを許可するようにしてもよい。
【００５７】
図４の処理によれば、受領したパスワードとディスク管理領域３００に記憶しているパスワード情報３０３が等しいときは（ステップＳ４０４でＹＥＳ）、セキュリティー機能を解除する（ステップＳ４０５）ので、正しいパスワードが入力されたときにのみ、セキュリティー機能を解除することができる。
【００５８】
図５は、図１における本体装置１００によって実行されるユーザ名読み出し処理のフローチャートである。
【００５９】
本処理は、本体装置１００の記憶装置１３０～１６０認識時、即ち本体装置１００の電源投入時又は記憶装置１３０～１６０への接続時に実行される。
【００６０】
図５において、本体装置１００は、記憶装置１３０～１６０を認識すると、記憶装置１３０～１６０の夫々のディスク管理領域３００から記憶装置種別情報３０１及びセキュリティー機能設定情報３０２をＲＡＭ１０３に読み出す（ステップＳ５０１）。
【００６１】

次いで、ＲＡＭ１０３に読み出した情報を参照して複数の記憶装置１３０～１６０の夫々について以下の処理を行う。

【００６２】

まず、記憶装置１３０～１６０のいずれか１つ（以下、単に「記憶装置」という）がセキュリティー機能付記憶装置であるか否かを判別し（ステップＳ５０２）、記憶装置がセキュリティー機能付記憶装置であるときは、セキュリティー機能が有効に設定されているか否かを判別し（ステップＳ５０３）、セキュリティー機能が有効に設定されているときは、ユーザにパスワードの入力を要求する表示を出力装置１２０に出力し（ステップＳ５０４）、入力装置１１０を介してパスワードが入力されると（ステップＳ５０５でＹＥＳ）、記憶装置にパスワードを送出し（ステップＳ５０６）、記憶装置のディスク管理領域３００からセキュリティー機能設定情報３０２をＲＡＭ１０３に読み出し（ステップＳ５０７）、セキュリティー機能設定情報３０２から、セキュリティー機能が解除されているか否かを判別し（ステップＳ５０８）、セキュリティー機能が解除されていないときは、ステップＳ５０４以降の処理を繰り返す一方、セキュリティー機能が解除されているときは、ユーザ情報領域３１０からユーザ名をＲＡＭ１０３に読み出し（ステップＳ５０９）、本処理を終了する。

【００６３】

ステップＳ５０３の判別の結果、セキュリティー機能が有効に設定されていないときは、ユーザ情報領域３１０からユーザ名をＲＡＭ１０３に読み出し（ステップＳ５０９）、本処理を終了する。

【００６４】

ステップＳ５０２の判別の結果、記憶装置がセキュリティー機能付記憶装置でないときは、直ちに本処理を終了する。

【００６５】

上述パスワード認証のスキームには、ハードディスク等の記憶装置のインターフェース規格として広く用いられているＡＴＡ／ＡＴＡＰＩ規格セキュリティー・モード・フィーチャー・セットにて規定されるスキームを利用してもよい。

【００６６】

図５の処理によれば、セキュリティー機能が解除されているときは（ステップＳ５０８でＹＥＳ）、ユーザ情報領域３１０からユーザ名をＲＡＭ１０３に読み出す（ステップＳ５０９）ので、正しいパスワードが入力され、セキュリティー機能が解除されたときにのみ、ユーザ名を読み出すことができる。

【００６７】

図６を用いて、図１の情報処理装置によって実行されるデータ移動・複写処理のフローチャートである。

【００６８】

図６において、本体装置１００は、ユーザにより入力装置１１０に入力されたデータの移動・複写要求を受領し（ステップＳ６０１）、図５のステップＳ５０１で記憶装置１３０～１６０認識時にディスク管理領域３００からＲＡＭ１０３上に読み出した記憶装置種別情報３０１を参照し、データの移動・複写元記憶装置がセキュリティー機能付記憶装置であるか否かを判別し（ステップＳ６０２）、データの移動・複写元記憶装置がセキュリティー機能付記憶装置でないときは、データの移動・複写を実行して（ステップＳ６０７）、本処理を終了する。

【００６９】

ステップＳ６０２の判別の結果、データの移動・複写元記憶装置がセキュリティー機能付記憶装置であるときは、図５のステップＳ５０１で読み出したセキュリティー設定情報３０１を参照し、データの移動・複写元記憶装置のセキュリティー機能が有効に設定されているか否かを判別し（ステップＳ６０３）、データの移動・複写元記憶装置のセキュリティー機能が有効に設定されていないときは、データの移動・複写を実行して（ステップＳ６０７）、本処理を終了する。

【００７０】
ステップＳ６０３の判別の結果、データの移動・複写元記憶装置のセキュリティー機能が有効に設定されているときは、図５のステップＳ５０１で読み出した記憶装置種別情報３０１を参照し、データの移動・複写先記憶装置がセキュリティー機能付記憶装置であるか否かを判別し（ステップＳ６０４）（セキュリティ情報比較手段）、データの移動・複写先記憶装置がセキュリティー機能付記憶装置でないときは、出力装置１２０に図７（ａ）の報知画面を表示し（表示手段）、データの移動・複写を禁止して（ステップＳ６０８）（データ移動制御手段）、本処理を終了する。
【００７１】
図７（ａ）において、報知画面は、データの移動・複写がセキュリティー機能付記憶装置からセキュリティー機能を持たない記憶装置への移動・複写であり、データのセキュリティーレベルを維持するために、データの移動・複写を許可しない旨をユーザに報知する。
【００７２】
ステップＳ６０４の判別の結果、データの移動・複写先記憶装置がセキュリティー機能付記憶装置であるときは、図５のステップＳ５０１で読み出したセキュリティー設定情報３０１を参照し、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されているか否かを判別し（ステップＳ６０５）、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されていないときは、出力装置１２０に図７（ｂ）の報知画面を表示し、データの移動・複写を禁止して（ステップＳ６０８）、本処理を終了する。
【００７３】
図７（ｂ）において、報知画面は、データの移動・複写がセキュリティー機能付記憶装置からセキュリティー機能が有効に設定されていない記憶装置への移動・複写であり、データのセキュリティーレベルを維持するために、データの移動・複写を許可しない旨をユーザに報知する。
【００７４】
ステップＳ６０５の判別の結果、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されているときは、図５のステップＳ５０１で読み出したユーザ名情報を参照し、データの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致しているか否かを判別し（ステップＳ６０６）、データの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していないときは、出力装置１２０に図７（ｃ）の報知画面を表示し、データの移動・複写を禁止して（ステップＳ６０８）、本処理を終了する。
【００７５】
図７（ｃ）において、報知画面は、データの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が異なるため、データの移動・複写を許可しない旨をユーザに報知する。
【００７６】
ステップＳ６０６の判別の結果、データの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致しているときは、データの移動・複写を実行して（ステップＳ６０７）、本処理を終了する。
【００７７】
図６の処理によれば、データの移動・複写先記憶装置がセキュリティー機能付記憶装置でないか（ステップＳ６０４でＮＯ）、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されていないか（ステップＳ６０５でＮＯ）、又はデータの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していないときは（ステップＳ６０６でＮＯ）、出力装置１２０に報知画面を表示し、データの移動・複写を禁止する（ステップＳ６０８）ので、ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができる。
【００７８】
図８は、図６のデータ移動・複写処理の変形例のフローチャートである。
【００７９】

図８の処理は、図６の処理と基本的に同じであり、図６のステップと同一のステップには同一符号を付してその説明を省略し、図６の処理と異なる部分についてのみ説明する。図８の処理は、ステップＳ６０８の代わりにステップＳ８０１～Ｓ８０３が配されている点でのみ図６のものと異なる。

【００８０】

ステップＳ６０４の判別の結果、データの移動・複写先記憶装置がセキュリティー機能付記憶装置でないときは、出力装置１２０に図９（ａ）の選択画面を表示する（ステップＳ８０１）（指示要求手段）。

【００８１】

図９（ａ）において、選択画面は、データの移動・複写がセキュリティー機能付記憶装置からセキュリティー機能を持たない記憶装置への移動・複写であり、データに対するセキュリティーレベルが低下する旨をユーザに警告し、データの移動・複写を行うか否かを、入力装置１１０を介してユーザに選択させる。

【００８２】

図８に戻り、ユーザが入力装置１１０によりデータの移動・複写を行うか否かの選択を行うと（ステップＳ８０２でＹＥＳ）（取得手段）、データの移動・複写を行うことが選択されたか否かを判別し（ステップＳ８０３）、データの移動・複写を行うことが選択されたときは、データの移動・複写を実行して（ステップＳ６０７）、データの移動・複写を行うことが選択されず、データの移動・複写を行わないことが選択されたときは、直ちに本処理を終了する。

【００８３】

ステップＳ６０５の判別の結果、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されていないときは、出力装置１２０に図９（ｂ）の選択画面を表示し（ステップＳ８０１）、ステップＳ８０２以降の処理を実行して、本処理を終了する。

【００８４】

図９（ｂ）において、選択画面は、データの移動・複写がセキュリティー機能付記憶装置からセキュリティー機能が有効に設定されていない記憶装置への移動・複写であり、データに対するセキュリティーレベルが低下する旨をユーザに警告し、データの移動・複写を行うか否かを、入力装置１１０を介してユーザに選択させる。

【００８５】

ステップＳ６０６の判別の結果、データの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していないときは、出力装置１２０に図９（ｃ）の選択画面を表示し（ステップＳ８０１）、ステップＳ８０２以降の処理を実行して、本処理を終了する。

【００８６】

図９（ｃ）において、選択画面は、データの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が異なる旨をユーザに警告し、データの移動・複写を行うか否かを、入力装置１１０を介してユーザに選択させる。

【００８７】

図８の処理によれば、データの移動・複写先記憶装置がセキュリティー機能付記憶装置でないか（ステップＳ６０４でＮＯ）、データの移動・複写先記憶装置のセキュリティー機能が有効に設定されていないか（ステップＳ６０５でＮＯ）、又はデータの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していないときは（ステップＳ６０６でＮＯ）、出力装置１２０に選択画面を表示し（ステップＳ８０１）、データの移動・複写を行うことが選択されたときは（ステップＳ８０３でＹＥＳ）、データの移動・複写を実行する（ステップＳ６０７）ので、ユーザによるデータの記憶装置間での移動・複写動作に対して強固な安全性を確保することができると共に、ユーザの意思を柔軟に反映してデータの移動・複写を行うことができる。

【００８８】

また、本発明の目的は、上記実施形態の機能を実現するソフトウェアのプログラムコードを記録した記憶媒体（又は記録媒体）を、システム又は装置に供給し、そのシステム又

は装置のコンピュータ（又はＣＰＵやＭＰＵ）が記憶媒体に格納されたプログラムコードを読出して実行することによっても達成されることは言うまでもない。

【００８９】

この場合、記憶媒体から読出されたプログラムコード自体が前述した実施の形態の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【００９０】

また、コンピュータが読出したプログラムコードを実行することにより、前述した実施の形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム(ＯＳ)などが実際の処理の一部又は全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれることは言うまでもない。

【００９１】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部又は全部を行い、その処理によって前述した実施の形態の機能が実現される場合も含まれることは言うまでもない。

【００９２】

また、上記プログラムは、上述した実施の形態の機能をコンピュータで実現することができればよく、その形態は、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給されるスクリプトデータ等の形態を有するものでもよい。

【００９３】

プログラムを供給する記録媒体としては、例えば、ＲＡＭ、ＮＶ－ＲＡＭ、フロッピー（登録商標）ディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＭＯ、ＣＤ－Ｒ、ＣＤ－ＲＷ、ＤＶＤ（ＤＶＤ－ＲＯＭ、ＤＶＤ－ＲＡＭ、ＤＶＤ－ＲＷ、ＤＶＤ＋ＲＷ）、磁気テープ、不揮発性のメモリカード、他のＲＯＭ等の上記プログラムを記憶できるものであればよい。又は、上記プログラムは、インターネット、商用ネットワーク、若しくはローカルエリアネットワーク等に接続される不図示の他のコンピュータやデータベース等からダウンロードすることにより供給される。

【図面の簡単な説明】

【００９４】

【図１】本発明の実施の形態に係る情報処理装置の構成を概略的に示すブロック図である。

【図２】図１における記憶装置１３０の内部構成を概略的に示すブロック図である。

【図３】図２の記憶装置１３０が有する記憶領域の構成を示す図である。

【図４】図２の記憶装置１３０によって実行されるセキュリティー機能解除処理のフローチャートである。

【図５】図１における本体装置１００によって実行されるユーザ名読み出し処理のフローチャートである。

【図６】図１の情報処理装置によって実行されるデータ移動・複写処理のフローチャートである。

【図７】図６のステップＳ６０８で表示される報知画面の一例を示す図であり、（ａ）はデータの移動・複写先記憶装置がセキュリティー機能付記憶装置でない場合、（ｂ）はデータの移動・複写先記憶装置のセキュリティー機能が有効に設定されていない場合、（ｃ）はデータの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していない場合を夫々示す。

【図８】図６のデータ移動・複写処理の変形例のフローチャートである。

【図９】図８のステップＳ８０１で表示される選択画面の一例を示す図であり、（ａ）はデータの移動・複写先記憶装置がセキュリティー機能付記憶装置でない場合、（ｂ）はデ

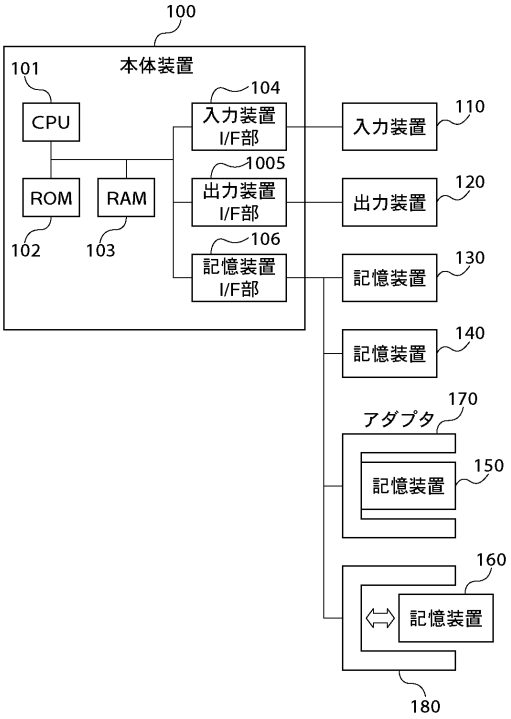
ータの移動・複写先記憶装置のセキュリティー機能が有効に設定されていない場合、（ｃ）はデータの移動・複写元記憶装置と移動・複写先記憶装置のユーザ名が一致していない場合を夫々示す。

【符号の説明】

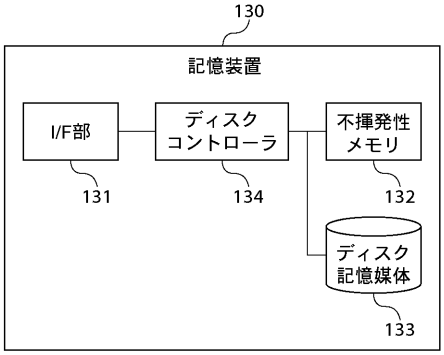
【００９５】

１００　本体装置
１０１　ＣＰＵ
１０２　ＲＯＭ
１０３　ＲＡＭ
１１０　入力装置
１２０　出力装置
１３０　記憶装置

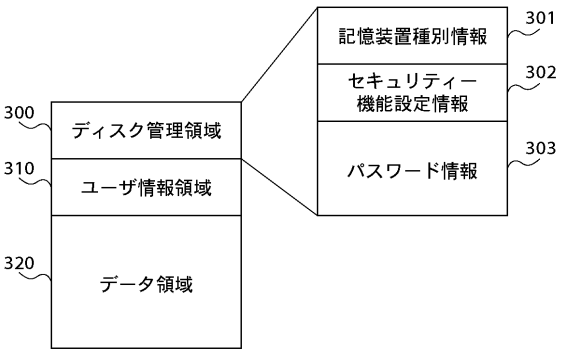
【図１】



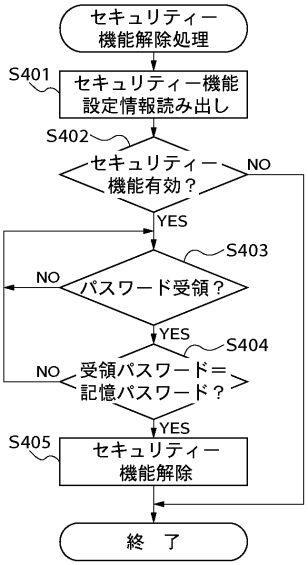
【図２】



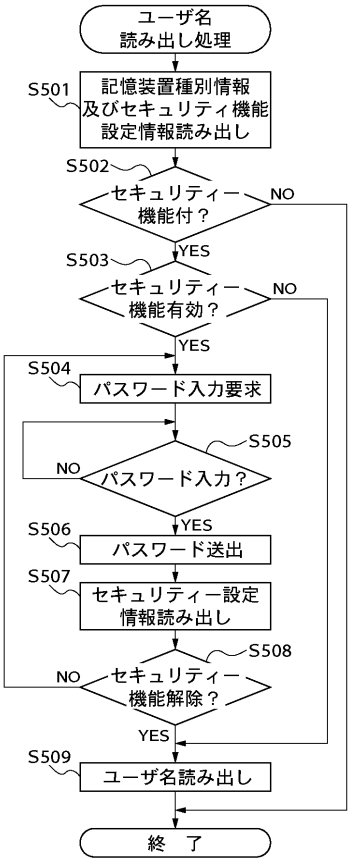
【図３】



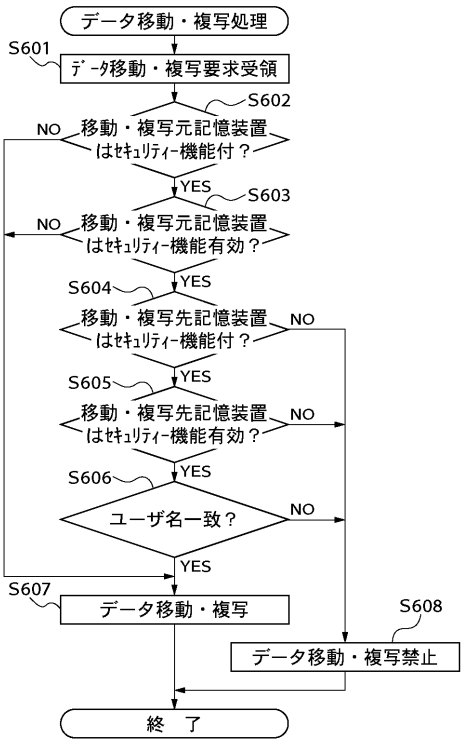
【図４】


セキュリティー
機能解除処理
S401
セキュリティー機能
設定情報読み出し
S402
セキュリティー
機能有効？
NO
YES
S403
パスワード受領？
NO
YES
S404
受領パスワード＝
記憶パスワード？
NO
YES
S405
セキュリティー
機能解除
終　了

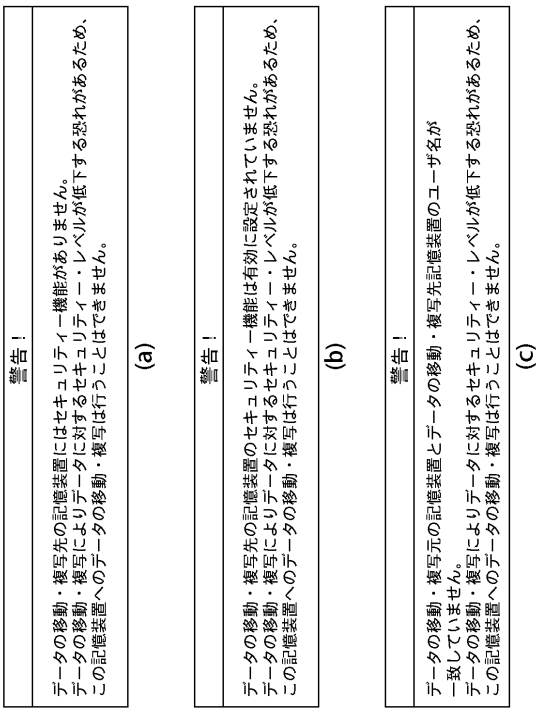
【図５】


ユーザ名
読み出し処理
S501
記憶装置種別情報
及びセキュリティ機能
設定情報読み出し
S502
セキュリティー
機能付？
NO
YES
S503
セキュリティー
機能有効？
NO
YES
S504
パスワード入力要求
S505
パスワード入力？
NO
YES
S506
パスワード送出
S507
セキュリティー設定
情報読み出し
S508
セキュリティー
機能解除？
NO
YES
S509
ユーザ名読み出し
終　了

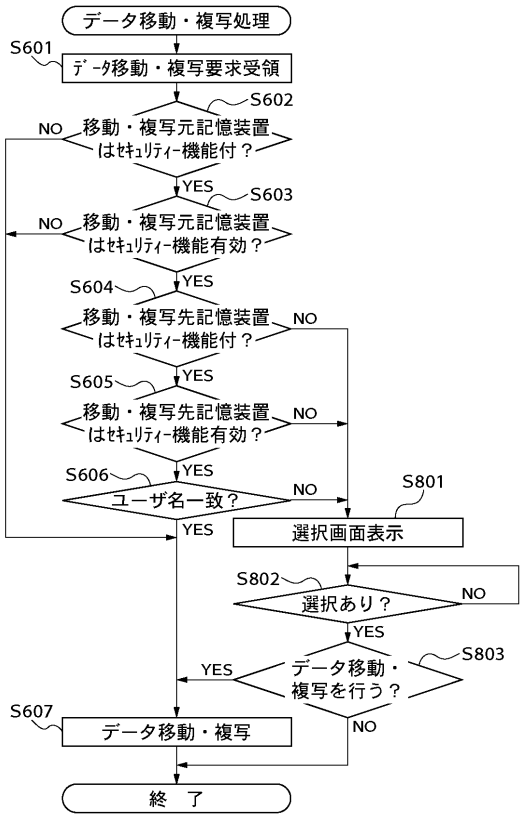
【図６】


データ移動・複写処理
S601
ﾃﾞｰﾀ移動・複写要求受領
S602
移動・複写元記憶装置
はｾｷｭﾘﾃｨｰ機能付？
NO
YES
S603
移動・複写元記憶装置
はｾｷｭﾘﾃｨｰ機能有効？
NO
YES
S604
移動・複写先記憶装置
はｾｷｭﾘﾃｨｰ機能付？
NO
YES
S605
移動・複写先記憶装置
はｾｷｭﾘﾃｨｰ機能有効？
NO
YES
S606
ユーザ名一致？
NO
YES
S607
データ移動・複写
S608
データ移動・複写禁止
終　了

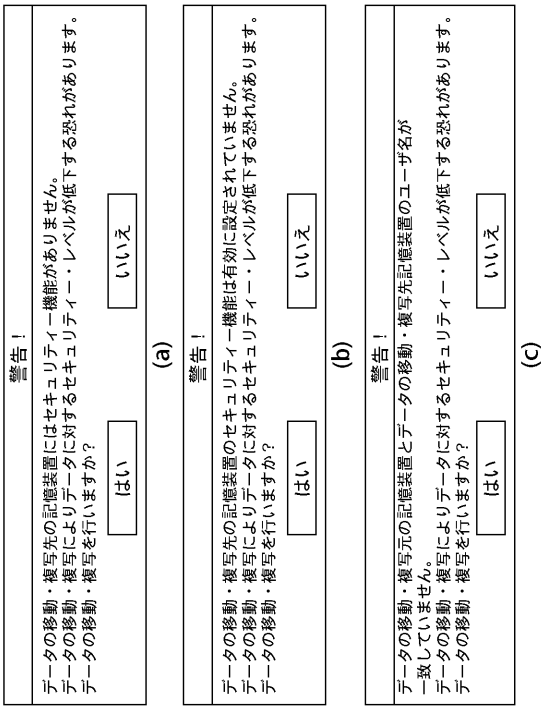
【図７】


警告！
データの移動・複写先の記憶装置にはセキュリティー機能がありません。
データの移動・複写によりデータに対するセキュリティー・レベルが低下する恐れがあるため、
この記憶装置へのデータの移動・複写は行うことはできません。
(a)
警告！
データの移動・複写先の記憶装置のセキュリティー機能は有効に設定されていません。
データの移動・複写によりデータに対するセキュリティー・レベルが低下する恐れがあるため、
この記憶装置へのデータの移動・複写は行うことはできません。
(b)
警告！
データの移動・複写元の記憶装置とデータの移動・複写先記憶装置のユーザ名が
一致していません。
データの移動・複写によりデータに対するセキュリティー・レベルが低下する恐れがあるため、
この記憶装置へのデータの移動・複写は行うことはできません。
(c)

【図８】


データ移動・複写処理
S601
ﾃﾞｰﾀ移動・複写要求受領
S602
移動・複写元記憶装置
はｾｷｭﾘﾃｨｰ機能付？
NO
YES
S603
移動・複写元記憶装置
はｾｷｭﾘﾃｨｰ機能有効？
NO
YES
S604
移動・複写先記憶装置
はｾｷｭﾘﾃｨｰ機能付？
NO
YES
S605
移動・複写先記憶装置
はｾｷｭﾘﾃｨｰ機能有効？
NO
YES
S606
ユーザ名一致？
NO
YES
S801
選択画面表示
S802
選択あり？
NO
YES
S803
データ移動・
複写を行う？
YES
NO
S607
データ移動・複写
終　了

【図９】


警告！
データの移動・複写先の記憶装置にはセキュリティー機能がありません。
データの移動・複写によりデータに対するセキュリティー・レベルが低下する恐れがあります。
データの移動・複写を行いますか？
はい
いいえ
(a)
警告！
データの移動・複写先の記憶装置のセキュリティー機能は有効に設定されていません。
データの移動・複写によりデータに対するセキュリティー・レベルが低下する恐れがあります。
データの移動・複写を行いますか？
はい
いいえ
(b)
警告！
データの移動・複写元の記憶装置とデータの移動・複写先記憶装置のユーザ名が
一致していません。
データの移動・複写によりデータに対するセキュリティー・レベルが低下する恐れがあります。
データの移動・複写を行いますか？
はい
いいえ
(c)

フロントページの続き

(72)発明者　外山　猛
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

Ｆターム(参考) 5B017 AA06　BA09　CA06　CA07　CA09