(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2009-223787
(P2009-223787A)
(43)公開日　平成21年10月1日(2009.10.1)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560D	5B017
G06F 3/06	(2006.01)	G06F	3/06	302A	5B065

審査請求 未請求　請求項の数 11　ＯＬ　（全 13 頁）

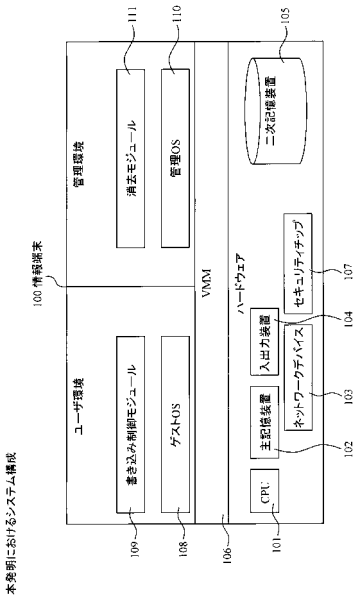
(21)出願番号　特願2008-69849(P2008-69849)
(22)出願日　平成20年3月18日(2008.3.18)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
東京都品川区東品川四丁目１２番７号
(74)代理人　100091096
弁理士　平木　祐輔
(74)代理人　100105463
弁理士　関谷　三男
(74)代理人　100102576
弁理士　渡辺　敏章
(74)代理人　100101063
弁理士　松丸　秀和

最終頁に続く

(54)【発明の名称】情報処理装置及び方法、並びにプログラム

(57)【要約】　（修正有）
【課題】二次記憶装置上にキャッシュされたデータをシャットダウン時に完全に消去し、残留データの悪用及び情報拡散を完全に防止することのできる機能を提供する。
【解決手段】利用者が使用するＯＳ上のアプリケーションによる二次記憶装置への書き込みを、ある特定のキャッシュ領域へリダイレクトしておき、前記利用者が使用するＯＳがシャットダウンした直後に、利用者が使用するＯＳとは隔離された環境で動作し、かつ、利用者からは直接操作できない正当な動作が保障されたＯＳ上から前記のある特定のキャッシュ領域を消去する。
【選択図】図１



【特許請求の範囲】
【請求項１】
不揮発性の二次記憶装置に対するアクセスを管理する情報処理装置であって、
前記二次記憶装置において、データの書込みが禁止される書込み禁止領域と、データの書込みは許される書込み許可領域とに分けて各領域を管理する領域管理手段と、
前記二次記憶装置への書込みが指示されたデータを前記書込み許可領域にのみ書込み処理する書込み制御手段と、
前記情報処理装置のシャットダウン時に、前記書込み許可領域に書き込まれたデータを消去するデータ消去手段と、
を備えることを特徴とする情報処理装置。
【請求項２】
さらに、前記情報処理装置のシャットダウンが発生したかを監視し、前記データ消去手段に前記シャットダウンの発生を通知する監視手段を備え、
前記データ消去手段は、前記監視手段による前記シャットダウンの通知に対応して前記書込み許可領域に書き込まれたデータを消去することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
不揮発性の二次記憶装置に対するアクセスを管理する情報処理装置であって、
前記二次記憶装置において、データの書込みが禁止される書込み禁止領域と、データの書込みは許されるが前記情報処理装置のシャットダウン時に書き込まれたデータが消去される消去予約領域とに分けて各領域を管理する領域管理手段と、
前記二次記憶装置への書込みが指示されたデータを前記消去予約領域にのみ書込み処理する書込み制御手段と、
を備えることを特徴とする情報処理装置。
【請求項４】
さらに、揮発性の主記憶装置を備え、
前記書込み制御手段は、前記二次記憶装置への書込みが指示されたデータをリダイレクトして前記主記憶装置に記憶し、前記主記憶装置に記憶できない場合に、前記書込み許可領域又は前記消去予約領域に前記書込み指示がされたデータを書き込むことを特徴とする請求項１乃至３に記載の情報処理装置。
【請求項５】
揮発性の主記憶装置と、不揮発性の二次記憶装置を有し、二次記憶装置に対するアクセスを制御する情報処理装置であって、
利用者が使用するＯＳとして動作するゲストＯＳ手段と、
前記ゲストＯＳ手段のバックグラウンドでＯＳとして動作する管理ＯＳ手段と、
前記ゲストＯＳ手段と前記管理ＯＳ手段を管理し、両者を同時に動作させるための仮想マシンモニタ手段と、
前記ゲストＯＳ手段上で動作する書込み制御手段と、
前記管理ＯＳ手段上で動作するデータ消去手段と、を備え、
前記書込み制御手段は、前記二次記憶装置において、データの書込みが禁止される書込み禁止領域と、データの書込みは許される書込み許可領域とに分けて各領域を管理し、前記二次記憶装置への書込みが指示されたデータを前記書込み許可領域にのみ書込み処理し、
前記データ消去手段は、前記ゲストＯＳ手段のシャットダウン時に、前記書込み許可領域に書き込まれたデータを消去することを特徴とする情報処理装置。
【請求項６】
前記仮想マシンモニタ手段は、前記ゲストＯＳ手段のシャットダウンが発生したかを監視し、前記管理ＯＳ手段に前記シャットダウンの発生を通知し、
前記管理ＯＳ手段は、前記仮想マシンモニタ手段による前記シャットダウンの通知に対応して、前記データ消去手段にデータの消去を指示し、

前記データ消去手段は、前記管理ＯＳ手段によるデータ消去の指示に応じて、前記書込み許可領域に書き込まれたデータを消去することを特徴とする請求項５に記載の情報処理装置。

【請求項７】

さらに、前記情報処理装置の起動時に、前記管理ＯＳ手段及び前記仮想マシンモニタ手段に改竄がなされていないかを確認するセキュリティチェック手段を備え、

前記管理ＯＳ手段及び前記仮想マシンモニタ手段に改竄がなされていない場合にのみ、利用者の前記ゲストＯＳ手段へのログインを可能とすることを特徴とする請求項５又は６に記載の情報処理装置。

【請求項８】

情報処理端末装置に含まれる不揮発性の二次記憶装置に対するアクセスを管理する情報処理方法であって、

領域管理手段が、前記二次記憶装置において、データの書込みが禁止される書込み禁止領域と、データの書込みは許される書込み許可領域とに分けて各領域を管理し、

書込み制御手段が、前記二次記憶装置への書込みが指示されたデータを前記書込み許可領域にのみ書込み処理し、

データ消去手段が、前記情報処理端末装置のシャットダウン時に、前記書込み許可領域に書き込まれたデータを消去する、ことを特徴とする情報処理方法。

【請求項９】

さらに、監視手段が、前記情報処理端末装置のシャットダウンが発生したかを監視し、前記データ消去手段に前記シャットダウンの発生を通知し、

前記データ消去手段が、前記監視手段による前記シャットダウンの通知に対応して前記書込み許可領域に書き込まれたデータを消去することを特徴とする請求項８に記載の情報処理方法。

【請求項１０】

前記書込み制御手段は、前記二次記憶装置への書込みが指示されたデータをリダイレクトして揮発性の主記憶装置に記憶し、前記主記憶装置に記憶できない場合に、前記書込み許可領域に前記書込み指示がされたデータを書き込むことを特徴とする請求項８又は９に記載の情報処理方法。

【請求項１１】

請求項８乃至１０の何れか１項に記載の情報処理方法をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、揮発性の主記憶装置と不揮発性の二次記憶装置を有し、二次記憶装置に対するアクセスを制御する情報処理装置及び方法、並びにプログラムに関する。

【背景技術】

【０００２】

ファイルサーバに保管されている重要データが利用者端末から拡散するのを防ぐためのシステムとして、シンクライアントシステムが考案されている。シンクライアントシステムは、端末内に不揮発性の二次記憶装置を装備しない端末（ディスクレスＰＣ）を使用するのが一般的であるが、書き込みを制御した不揮発性の二次記憶装置を備えるＰＣをシンクライアント端末として使用するシステムも存在する。

【０００３】

しかし、二次記憶装置を装備しない端末を使ったシンクライアントシステムでは、専用サーバやブレード、及び、高速なネットワークの存在が前提となるため、新たにシステムを構築する際、インフラ設備に莫大なコストがかかる問題がある。

【０００４】

このようなシンクライアントの問題を解決するために、例えば、特許文献１では、二次

記憶装置（不揮発性メモリ）を持つ端末において、アプリケーションから二次記憶装置へ書き込みが発生した場合、その書き込みを主記憶装置（揮発性メモリ）上へリダイレクトすることで、二次記憶装置への書き込みを制限し、擬似的に二次記憶を持たない端末を実現している。これらのシステムによれば、ファイルサーバに保管されている重要データが拡散するのを防止することに加え、利用者による不適切なＯＳ設定変更や、アプリケーションのインストールを防止することも可能である。

【０００５】

また、特許文献１のシステムは、不揮発性の二次記憶装置への書き込みを、揮発性の主記憶装置中にリダイレクトすることで、二次記憶装置への書き込みを制限している。もし主記憶装置上の容量が不足した場合は、二次記憶装置上の暗号スワップ領域へデータをスワップする。そして、暗号鍵を揮発性の主記憶装置上へ保存しておき、シャットダウンと同時に暗号鍵が自動で消去され暗号スワップ領域のキャッシュデータが使用不能となることを想定して、残留データの悪用及び情報拡散を防止している。

【０００６】

【特許文献１】特開２００７－１７２０６３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、特許文献１に示されるシステムおいては、暗号化されているとはいえ不揮発性の二次記憶装置上にデータが残ることは問題である。なぜなら、暗号化は破られる可能性があり、破られ難くすればパフォーマンスが著しく低下するためである。単純な解決策として、スワップデータを消去するモジュールを組み込むことが考えられるが、ＯＳがクラッシュしてしまった場合は消去の保障はできない。そこで、シャットダウン時に不揮発性の二次記憶装置上のキャッシュデータを完全消去するための手段が必要となってくる。

【０００８】

本発明はこのような状況に鑑みてなされたものであり、二次記憶装置上にキャッシュされたデータをシャットダウン時に完全に消去し、残留データの悪用及び情報拡散を完全に防止することのできる機能を開示するものである。

【課題を解決するための手段】

【０００９】

上記課題を解決するために、本発明では、不揮発性の二次記憶装置を備える情報端末において、シャットダウン時に端末上にキャッシュされたデータを確実に消去するための機能を開示している。

【００１０】

本発明における情報端末の構成は、一般的な情報端末が備えるＣＰＵ、主記憶装置、入出力装置、ネットワークデバイス、二次記憶装置の他に、利用者が使用するＯＳ（以後、ゲストＯＳと呼ぶ）と、ゲストＯＳのバックグラウンドで動作するＯＳ（以後、管理ＯＳと呼ぶ）が同時に動作できるための仮想化ハードウェア環境を備え、かつ、管理ＯＳ及び管理ＯＳ上で動作するアプリケーションが不正改竄されていないことを保障するセキュリティチップを備える。前記ＣＰＵは仮想化に対応した設計になっている場合も考えられる。ゲストＯＳ内には書き込み制御モジュールが備わっており、ゲストＯＳによる二次記憶装置への書き込みを、特定のキャッシュ領域にリダイレクトする。また、管理ＯＳ内には、消去モジュールが備わっており、端末のシャットダウン時に前記特定のキャッシュ領域を消去する。

【００１１】

この時、ゲストＯＳと管理ＯＳは別パーティションで区切られており、互いの動作は影響しないため、ゲストＯＳ上で何らかの問題が起きた場合でも、管理ＯＳ上の消去モジュールによる特定のキャッシュ領域の消去は保障される。

【００１２】

即ち、本発明は、不揮発性の二次記憶装置に対するアクセスを管理する情報処理装置に関し、二次記憶装置において、データの書込みが禁止される書込み禁止領域と、データの書込みは許される書込み許可領域とに分けて各領域を管理する領域管理手段と、二次記憶装置への書込みが指示されたデータを書込み許可領域にのみ書込み処理する書込み制御手段と、情報処理装置のシャットダウン時に、書込み許可領域に書き込まれたデータを消去するデータ消去手段と、を備えている。当該情報処理装置は、さらに、情報処理装置のシャットダウンが発生したかを監視し、データ消去手段にシャットダウンの発生を通知する監視手段を備える。そして、データ消去手段は、監視手段によるシャットダウンの通知に対応して書込み許可領域に書き込まれたデータを消去する。当該情報処理装置は、さらに、揮発性の主記憶装置を備え、書込み制御手段は、二次記憶装置への書込みが指示されたデータをリダイレクトして主記憶装置に記憶し、主記憶装置に記憶できない場合に、書込み許可領域に書込み指示がされたデータを書き込む。

【００１３】

また、本発明による情報処理装置は、揮発性の主記憶装置と、不揮発性の二次記憶装置を有し、二次記憶装置に対するアクセスを制御する情報処理装置に関し、利用者が使用するＯＳとして動作するゲストＯＳ手段と、ゲストＯＳ手段のバックグラウンドでＯＳとして動作する管理ＯＳ手段と、ゲストＯＳ手段と管理ＯＳ手段を管理し、両者を同時に動作させるための仮想マシンモニタ手段と、ゲストＯＳ手段上で動作する書込み制御手段と、管理ＯＳ手段上で動作するデータ消去手段と、を備える。そして、書込み制御手段は、二次記憶装置において、データの書込みが禁止される書込み禁止領域と、データの書込みは許される書込み許可領域とに分けて各領域を管理し、二次記憶装置への書込みが指示されたデータを書込み許可領域にのみ書込み処理し、データ消去手段は、ゲストＯＳ手段（情報処理装置）のシャットダウン時に、書込み許可領域に書き込まれたデータを消去する。なお、仮想マシンモニタ手段は、ゲストＯＳ手段のシャットダウンが発生したかを監視し、前記管理ＯＳ手段に前記シャットダウンの発生を通知し、管理ＯＳ手段は、仮想マシンモニタ手段によるシャットダウンの通知に対応して、データ消去手段にデータの消去を指示する。そして、データ消去手段は、管理ＯＳ手段によるデータ消去の指示に応じて、書込み許可領域に書き込まれたデータを消去する。当該情報処理装置は、さらに、情報処理装置（ゲストＯＳ手段）の起動時に、管理ＯＳ手段及び仮想マシンモニタ手段に改竄がなされていないかを確認するセキュリティチェック手段を備える。管理ＯＳ手段及び仮想マシンモニタ手段に改竄がなされていない場合にのみ、利用者のゲストＯＳ手段へのログインを可能とする。

【００１４】

本発明は、さらに、上述の情報処理装置に対応する方法及びプログラムも提供する。

【００１５】

さらなる本発明の特徴は、以下本発明を実施するための最良の形態および添付図面によって明らかになるものである。

【発明の効果】

【００１６】

本発明によれば、情報処理装置内のデータの悪用及び情報拡散を完全に防止することができるようになる。

【発明を実施するための最良の形態】

【００１７】

本発明は、二次記憶装置を備える情報端末において、利用者による不適切な設定変更、データ保存、アプリケーションのインストールを防止し、かつ、シャットダウン時に端末上にキャッシュされたデータを確実に消去することで残留データの悪用を防止しつつ情報端末を速やかに起動時の状態に戻すことを可能にする機能に関するものである。

【００１８】

以下、添付図面を参照して本発明の実施形態について説明する。ただし、本実施形態は本発明を実現するための一例に過ぎず、本発明の技術的範囲を限定するものではないこと

に注意すべきである。また、各図において共通の構成については同一の参照番号が付されている。

【００１９】

＜装置の構成＞

図１は、本発明の実施形態による情報漏洩防止装置（情報端末装置１００）の概略構成を示す図である。

【００２０】

情報端末装置１００は、一般的な情報端末が備えるＣＰＵ１０１と、揮発性のメモリである主記憶装置１０２と、ネットワークデバイス１０３と、キーボードやマウス、並びにプリンタやディスプレイ等で構成される入出力装置１０４と、不揮発性のメモリである二次記憶装置１０５を備える。また、情報端末装置１００は、その他に、利用者が使用するＯＳ（以後、ゲストＯＳと呼ぶ）１０８と、ゲストＯＳのバックグラウンドで動作するＯＳ（以後、管理ＯＳと呼ぶ）１１０と、それら２つのＯＳが同時に動作させるための仮想マシン・モニタ（以後、ＶＭＭ：Ｖｉｒｔｕａｌ Ｍａｃｈｉｎｅ Ｍｏｎｉｔｏｒと呼ぶ）１０６を備え、かつ、管理ＯＳ及び管理ＯＳ上で動作するアプリケーションが不正改竄されていないことを保障するセキュリティチップ１０７を備えている。

【００２１】

セキュリティチップ（例えば、現状のＴＰＭ（Ｔｒｕｓｔｅｄ Ｐｌａｔｆｏｒｍ Ｍｏｄｕｌｅ）に相当）１０７とは、ハードウェア耐タンパ性をもつセキュリティチップである。そして、セキュリティチップ１０７は、暗号演算やハッシュ演算といった演算機能と、暗号鍵やハッシュ値を格納する機能を備え、ＣＰＵ１０１から独立して暗号化・復号化・署名作成・検証が可能となっている。本情報端末装置１００におけるセキュリティチップ１０７の主な動作は、端末起動時に管理ＯＳ（後述）および管理ＯＳ１１０上で動作するアプリケーションのバイナリデータの署名検証を行い、それらが正常に動作することを保障することである。つまり、セキュリティチップ１０７は、情報端末装置１００の起動時に完全性検証を行うものである。

【００２２】

管理ＯＳ１１０は、基本的に利用者による操作はできないＯＳであり、かつ、ゲストＯＳ１０８（後述）とは分離したパーティション上で動作する。また、端末起動時にはセキュリティチップ１０７によるバイナリイメージの完全性検証がなされているため、端末起動からシャットダウンまでの間、管理ＯＳ１１０は安全に動作することが保障されている。さらに、管理ＯＳ１１０は、端末起動時点からシャットダウンまで、ゲストＯＳ１０８のバックグラウンドで動作している。また、管理ＯＳ１１０上には、消去モジュール１１１がインストールされている（詳細は後述）。

【００２３】

ゲストＯＳ１０８は、利用者が実際に操作できるＯＳである。つまり、利用者はゲストＯＳ１０８上でインターネットやドキュメント作成等を行う。利用者が情報端末装置１００の電源をＯＮにした場合、利用者にはゲストＯＳ１０８のみ起動しているように見える。また、ゲストＯＳ１０８上には書き込み制御モジュール１０９がインストールされている（詳細は後述）。

【００２４】

ＶＭＭ１０６は、管理ＯＳ１１０とゲストＯＳ１０８を同時に動作させるために、ＣＰＵ１０１や主記憶装置１０２等のリソースの割り振りを管理するモジュールである。ゲストＯＳ１０８と管理ＯＳ１１０はＶＭＭ上で動作するＯＳであり、ゲストＯＳ１０８が起動する前にＶＭＭ１０６及び管理ＯＳ１１０がバックグラウンドで起動する。ゲストＯＳ１０８の起動・停止・シャットダウン等はＶＭＭ１０６により管理（監視）されている。

【００２５】

書き込み制御モジュール１０９は、ゲストＯＳ１０８上で動作するモジュールである。この書込み制御モジュール１０９は、ゲストＯＳ１０８が占有する二次記憶装置１０５の領域を、消去予約領域３０３と書き込み制御領域３０２（図３参照）の２つの領域に分割

管理する機能を有する。また、書込み制御モジュール１０９は、ゲストＯＳ１０８上のアプリケーション３０４（図３参照）から二次記憶装置１０５への書き込み指示があった場合に、書き込み制御領域３０２に書き込まれるデータを全て消去予約領域３０３にリダイレクト・キャッシュする機能を備えている。

【００２６】

ここで、書き込み制御領域３０２とは、ＯＳ及びアプリケーションが動作するために必要なデータが記憶されている領域である。この書き込み領域３０２は、利用者が操作した場合に発生する二次記憶装置３０２への書き込みからは保護されている。また、消去予約領域３０３とは、書き込み制御モジュール１０９によりリダイレクトされてキャッシュされる領域であり、情報端末装置１００がシャットダウンされる時に管理ＯＳ１１０上の消去モジュール１１１（後述）により完全消去される記憶領域である。

【００２７】

消去モジュール１１１は、管理ＯＳ１１０上で動作するモジュールであり、情報端末装置１００をシャットダウンしたときに、ゲストＯＳ１０８が管理する二次記憶装置１０５内の消去予約領域データを消去する機能を備える。実際には、管理ＯＳ１１０がＶＭＭ１０６からゲストＯＳ１０８のシャットダウン通知を受けとった後、ゲストＯＳ１０８が管理する二次記憶装置１０５上のボリューム領域をマウントし、消去予約領域３０３をゼロクリアする。

【００２８】

＜情報端末装置の起動の動作＞

図２は、情報端末装置を起動する処理を説明するためのフローチャートである。なお、ＶＭＭ１０６及び管理ＯＳ１１０のインストールイメージは二次記憶装置１０５上ではなく、専用の不揮発性の主記憶装置等に保存されている場合もある。また、ここでは事前に正しい動作をしている場合のバイナリイメージのハッシュ値をセキュリティチップ１０７に保存してあることが前提となっている。

【００２９】

まず、情報端末装置１００が起動（例えば、利用者によって電源がＯＮされる）する（ステップＳ２００）と、セキュリティチップ１０７は、自身の署名検証機能を使ってＶＭＭ１０６の完全性検証を実行する（ステップＳ２０１）。例えば、セキュリティチップ１０７は、自身に保存されているＶＭＭ１０６のバイナリイメージのハッシュ値（これは、あらかじめ正常な動作が保障されているイメージのハッシュ値）と、現在のＶＭＭ１０６のバイナリイメージのハッシュ値とを比較する。ＶＭＭ１０６の改竄が行われていないことが確認できた後、処理はステップＳ２０２に移行する。

【００３０】

次に、セキュリティチップ１０７は、管理ＯＳ１１０の完全性検証を実行する（ステップＳ２０２）。この検証も、例えばＶＭＭ１０６の場合と同様に、ハッシュ値の比較によって行われる。

【００３１】

ＶＭＭ１０６と管理ＯＳ１１０の両方とも改竄されていないことが確認できた場合のみ、ＣＰＵ１０１は、セキュリティチップ１０７からＶＭＭ１０６と管理ＯＳ１１０を起動する（ステップＳ２０３）。改竄が検知された場合、情報端末装置１００の起動処理は終了する。この場合、正常なＶＭＭ１０６及び管理ＯＳ１１０をインストールする必要がある。

【００３２】

管理ＯＳ１１０が起動すると、ＶＭＭ１０６はゲストＯＳ１０８へ起動信号を送り、ＣＰＵ１０１は、ゲストＯＳ１０８を起動する（ステップＳ２０４）。ゲストＯＳ１０８の起動後、管理ＯＳ１１０は、ゲストＯＳ１０８の起動・シャットダウンをＶＭＭ１０６からの通知を基に監視する（ステップＳ２０５）。

【００３３】

そして、ゲストＯＳ１０８が起動された後、利用者はゲストＯＳ１０８にログインし、

ＰＣを使用することが可能な状態となる（ステップＳ２０６）。この時、管理ＯＳ１１０はゲストＯＳ１０８のバックグラウンドで動作中であるが、ＶＭＭ１０６により両者は隔離されているため、ゲストＯＳ１０８が停止した場合でも管理ＯＳ１１０の動作が停止することはない。

【００３４】

＜書き込みモジュールの動作＞

図３は、書き込み制御モジュールの動作の概略を説明するための図である。動作の前提として、ゲストＯＳ１０８には、二次記憶装置１０５上のゲストＯＳパーティション３０１の領域が割り当てられているものとする。なお、この割り当ては、ＶＭＭ１０６のリソース管理機能が行っている。

【００３５】

図３に示されるように、ゲストＯＳ１０８上にインストールされている書き込み制御モジュール１０９は、ゲストＯＳパーティション３０１を書き込み制御領域３０２と消去予約領域３０３に分割して管理する。ゲストＯＳ１０８上において利用者の操作により、アプリケーション３０４が書き込み制御領域３０２に書き込みを行おうとした場合、消去予約領域３０３にリダイレクトされ、書き込むべきデータがキャッシュされる。以上の動作により、書き込み制御領域３０２のデータは完全に保護され、利用者による不適切な設定変更やアプリケーション３０４のインストールを制限することが可能となる。

【００３６】

なお、書込み処理に関し、二次記憶装置への書込み指示がなされた場合、まず主記憶装置１０２にデータ書込みをリダイレクトし、主記憶装置が一杯になってデータを格納できなくなった場合に、消去予約領域３０３に書込み処理を実行するようにしてもよい。主記憶装置１０２は揮発性メモリなので、シャットダウン時には格納されたデータは全て消去されるのでデータセキュリティを保つことができる。また、主記憶装置１０２が一杯になっても消去予約領域３０３に格納されたデータもシャットダウン時に確実に消去されるのでデータのセキュリティを確保することができる。このように、主記憶領域１０２に格納できなくなった場合でもデータ漏洩を確実に防止することができるようになる。

【００３７】

また、本実施形態では、書き込み制御モジュール１０９は、情報端末装置１００内のファイルシステム（図示せず）の下位レイヤ、かつ、二次記憶装置１０５及び主記憶装置１０２の上位レイヤに設けられるようにしてもよい。このように、ファイルシステムと二次記憶装置１０５及び主記憶装置１０２との間にフィルタドライバを配置することにより、ファイルシステムに対しては、データの書込みが二次記憶装置１０５に行われていると見せかけることができ、矛盾無くＯＳが実行される状態にされる。このように、ファイルシステムより下のレイヤで書込みデータを主記憶装置１０２中にキャッシュする。これにより、主記憶装置１０２の格納容量が一杯になっていない場合には、ＯＳにはあたかも二次記憶装置１０５にファイル保存をしているかのように見せつつ、実際には物理的に二次記憶装置１０５への書込みを禁止する。以上の仕組みにより、ＯＳ実行時に必要なデータの書込みを阻害することがなく、二次記憶装置１０５への書込みを禁止していても、通常通りにＯＳを動作させることが可能となる。また、二次記録装置１０５内のデータ自体を改竄することができなくなるので、データの機密性も保つことができる。

【００３８】

図４は、利用者がゲストＯＳ１０８にログインした後、通常操作、例えば、メールやドキュメント作成等の操作を行ったときに、アプリケーション３０４から二次記憶装置１０５へのアクセスが発生した場合の、書き込み制御モジュール１０９の書き込み・読み込み動作を説明するためのフローチャートである。

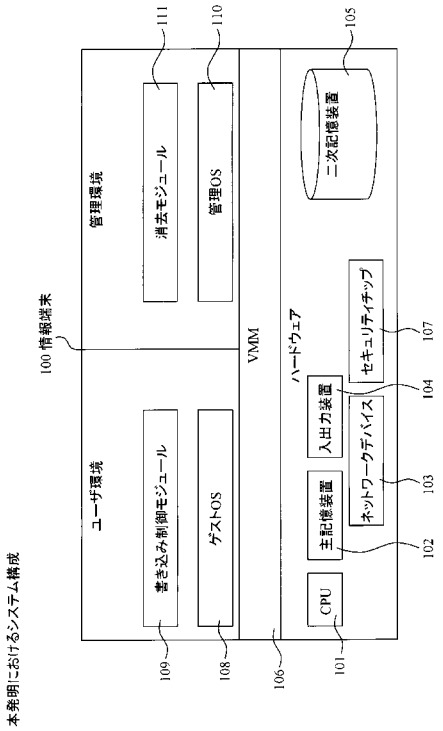
【００３９】

アプリケーション３０４やＯＳ（ゲストＯＳ１０８）が二次記憶装置１０５へのアクセスを行った場合（ステップＳ４００）、書き込み制御モジュール１０９は、そのアクセスが書き込み処理か読み込み処理かを判断する（ステップＳ４０１）。

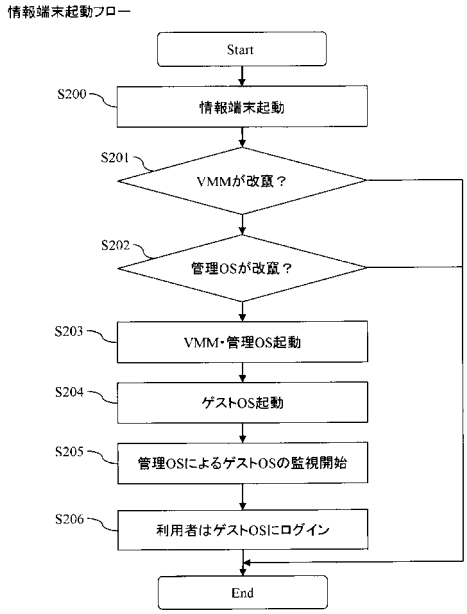
【００４０】
上記アクセスが書き込み処理の場合、書き込み制御モジュール１０９は、消去予約領域３０３に書き込むべきデータをキャッシュする（ステップＳ４０５）。一方、上記アクセスが読み込み処理の場合、書き込み制御モジュール１０９は、消去予約領域３０３に読み込むべきキャッシュデータがあるかどうかを判断する（ステップＳ４０２）。
【００４１】
読み込むべきキャッシュデータがあると判断された場合は、書き込む制御モジュール１０９は、そのまま消去予約領域３０３からデータを読み込む（ステップＳ４０３）。一方、キャッシュデータがない場合、書き込み制御モジュール１０９は、二次記憶装置１０５の書き込み制御領域３０３からデータを読み込む（ステップＳ４０４）。
【００４２】
＜情報端末装置のシャットダウン時の動作＞
図５は、情報端末装置１００をシャットダウンするときの管理ＯＳ１１０による消去予約領域３０４の消去動作を説明するためのフローチャートである。
【００４３】
利用者が、ゲストＯＳ１０８上から情報端末装置１００のシャットダウンを実行すると（ステップＳ５００）、ゲストＯＳ１０８は二次記憶装置１０５上での割り当て領域、つまり、ゲストＯＳパーティション領域３０１をアンマウントする（ステップＳ５０１）。つまり、ゲストＯＳ１０８は、ゲストＯＳパーティション領域３０１を認識（管理）状態から切り離す。
【００４４】
その後、ＶＭＭ１０６は、ゲストＯＳ１０８からシャットダウン通知を受けとる（ステップＳ５０２）と、ゲストＯＳ１０８がシャットダウンしたことを管理ＯＳ１１０に通知する（ステップＳ５０３）。
【００４５】
管理ＯＳ１１０は、このゲストＯＳ１０８のシャットダウン通知を受けた後、ゲストＯＳ１０８が使用していたゲストＯＳパーティション領域３０１をマウントする（ステップＳ５０４）。つまり、管理ＯＳ１１０は、ゲストＯＳパーティション領域３０１（書き込み制御領域３０２と消去予約領域３０３）を認識する。当該領域をマウント後、管理ＯＳ１１０は、消去モジュール１１１に消去予約領域３０３のキャッシュデータの消去を命令する。すると、消去モジュール１１１は、消去予約領域３０３をゼロクリアして新規に作成されたローカルデータを完全削除する（ステップＳ５０５）。その後、ＣＰＵ１０１は、情報端末装置１００をシャットダウンする。
【００４６】
なお、管理ＯＳ１１０の動作は、予め完全性検証により保障されているため、及び、管理ＯＳ１１０とゲストＯＳ１０８が、二次記憶装置１０５において別パーティション領域で動作しているため、たとえゲストＯＳ１０８が何らかの原因でクラッシュしても、消去予約領域３０３にキャッシュデータが残ることはない。以上により、消去予約領域に書き込まれたデータを完全かつ安全に削除することが可能となり、当該データの悪用及び情報拡散を防止することができるようになる。
【００４７】
なお、本発明は、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によっても実現できる。この場合、プログラムコードを記録した記憶媒体をシステム或は装置に提供し、そのシステム或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み出す。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施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自体、及びそれを記憶した記憶媒体は本発明を構成することになる。このようなプログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－Ｒ、磁気テープ、不揮発性のメモリカード、ＲＯＭなどが用いられる。

【００４８】
　また、プログラムコードの指示に基づき、コンピュータ上で稼動しているＯＳ（オペレーティングシステム）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ようにしてもよい。さらに、記憶媒体から読み出されたプログラムコードが、コンピュータ上のメモリに書きこまれた後、そのプログラムコードの指示に基づき、コンピュータのＣＰＵ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ようにしてもよい。
【００４９】
　また、実施の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ネットワークを介して配信することにより、それをシステム又は装置のハードディスクやメモリ等の記憶手段又はＣＤ-ＲＷ、ＣＤ-Ｒ等の記憶媒体に格納し、使用時にそのシステム又は装置のコンピュータ(又はＣＰＵやＭＰＵ)が当該記憶手段や当該記憶媒体に格納されたプログラムコードを読み出して実行するようにしても良い。
【図面の簡単な説明】
【００５０】
【図１】本発明による情報漏洩防止装置（情報端末装置）の概略構成を示す図である。
【図２】情報端末装置の起動時の動作を説明するためのフローチャートである。
【図３】書き込み制御モジュールの動作図である。
【図４】書き込み制御モジュールの書き込み・読み込み処理を説明するためのフローチャートである。
【図５】シャットダウン時の管理ＯＳにおける消去予約領域の消去動作を説明するためのフローチャートである。
【符号の説明】
【００５１】
１００…情報端末装置、１０１…ＣＰＵ、１０２…主記憶装置、１０３…ネットワークデバイス、１０４…入出力装置、１０５…二次記憶装置、１０６…ＶＭＭ、１０７…セキュリティチップ、１０８…ゲストＯＳ、１０９…書き込み制御モジュール、１１０…管理ＯＳ、１１１…消去モジュール

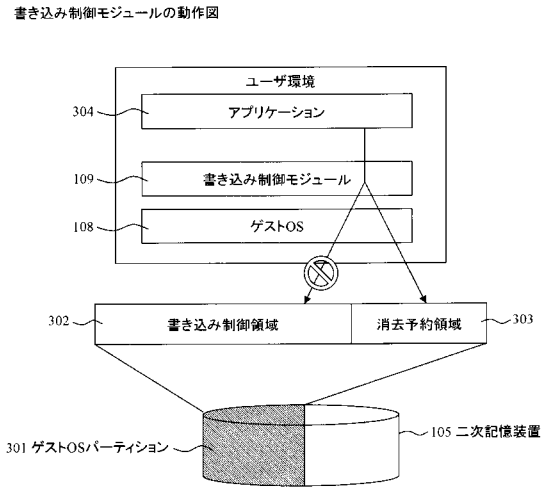
【図１】


本発明におけるシステム構成
100 情報端末
管理環境
ユーザ環境
消去モジュール
管理OS
書き込み制御モジュール
ゲストOS
VMM
ハードウェア
二次記憶装置
セキュリティチップ
入出力装置
ネットワークデバイス
主記憶装置
CPU
111
110
105
107
104
103
102
101
106
109
108

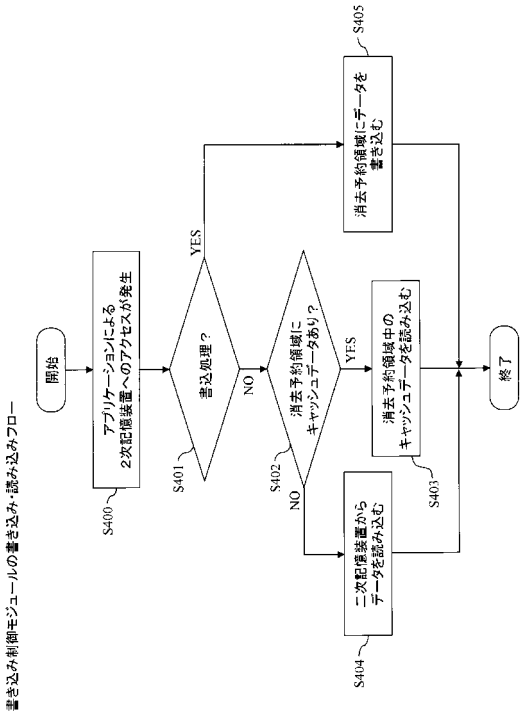
【図２】


情報端末起動フロー
Start
S200
情報端末起動
S201
VMMが改竄？
S202
管理OSが改竄？
S203
VMM・管理OS起動
S204
ゲストOS起動
S205
管理OSによるゲストOSの監視開始
S206
利用者はゲストOSにログイン
End

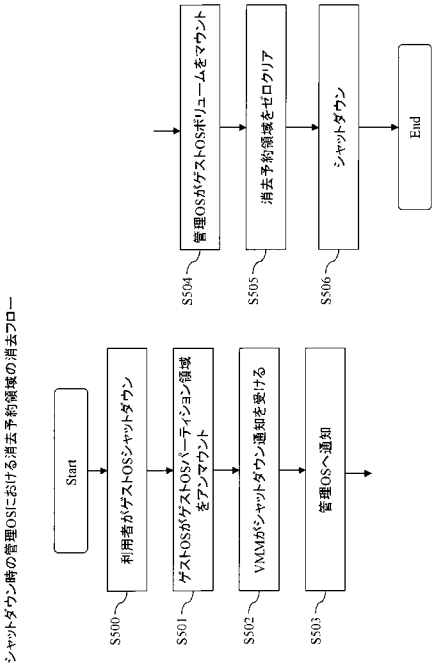
【図３】


書き込み制御モジュールの動作図
ユーザ環境
304
アプリケーション
109
書き込み制御モジュール
108
ゲストOS
302
書き込み制御領域
消去予約領域
303
301 ゲストOSパーティション
105 二次記憶装置

【図４】


書き込み制御モジュールの書き込み・読み込みフロー
開始
S400
アプリケーションによる
2次記憶装置へのアクセスが発生
S401
書込処理？
YES
NO
S402
消去予約領域に
キャッシュデータあり？
YES
NO
S403
消去予約領域中の
キャッシュデータを読み込む
S404
二次記憶装置から
データを読み込む
S405
消去予約領域にデータを
書き込む
終了

【図５】


シャットダウン時の管理OSにおける消去予約領域の消去フロー
Start
利用者がゲストOSシャットダウン
S500
ゲストOSがゲストOSパーティション領域をアンマウント
S501
VMMがシャットダウン通知を受ける
S502
管理OSへ通知
S503
管理OSがゲストOSボリュームをマウント
S504
消去予約領域をゼロクリア
S505
シャットダウン
S506
End

フロントページの続き

(72)発明者　中山　晃治
東京都品川区東品川四丁目１２番７号　日立ソフトウエアエンジニアリング株式会社内

Ｆターム(参考) 5B017 AA07　BA08　CA06　CA16
5B065 CH02