(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7141663号
(P7141663)

(45)発行日　令和4年9月26日(2022.9.26)

(24)登録日　令和4年9月14日(2022.9.14)

(51)国際特許分類
Ｇ０６Ｆ　21/57　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/57　３５０

請求項の数　9　（全14頁）

(21)出願番号　特願2020-573513(P2020-573513)
(86)(22)出願日　平成31年3月15日(2019.3.15)
(65)公表番号　特表2021-530776(P2021-530776A)
(43)公表日　令和3年11月11日(2021.11.11)
(86)国際出願番号　PCT/CN2019/078366
(87)国際公開番号　WO2020/001078
(87)国際公開日　令和2年1月2日(2020.1.2)
審査請求日　令和2年12月25日(2020.12.25)
(31)優先権主張番号　201810662749.0
(32)優先日　平成30年6月25日(2018.6.25)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　520512568
湖南国科微電子股▲ふん▼有限公司
ＨＵＮＡＮ ＧＯＫＥ ＭＩＣＲＯＥＬＥＣＴＲＯＮＩＣＳ ＣＯ．，ＬＴＤ．
中華人民共和国４１０１３１湖南省長沙市長沙経済技術開発区東十路南段９号
(74)代理人　100121728
弁理士　井関 勝守
(74)代理人　100165803
弁理士　金子 修平
(74)代理人　100170900
弁理士　大西 渉
(72)発明者　楊 萬雲
中華人民共和国４１０１３１湖南省長沙市長沙経済技術開発区東十路南段９号

最終頁に続く

(54)【発明の名称】　記憶データ安全動作方法及びシステム

(57)【特許請求の範囲】
【請求項１】
ホストが第１記憶装置が検出された時に、前記第１記憶装置に予め記憶された安全管理プログラムをロードすることと、
ホストが安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得することと、
ホストが暗号化の身分情報を前記第１記憶装置に送信することと、
ホストが前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づいてオペレーティングシステムを動作することと、を含み、
安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得することは、
安全管理プログラムを動作して第２記憶装置を検出し、前記第２記憶装置が検出された時に前記第２記憶装置に予め記憶された暗号化の身分情報を読み取ること、を含み、
前記第２記憶装置は、挿抜可能な記憶装置とする
ことを特徴とする記憶データ安全動作方法。
【請求項２】
安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得することは、
安全管理プログラムを動作してホストに予め記憶された暗号化の身分情報を読み取ること、を含む
ことを特徴とする請求項１に記載の記憶データ安全動作方法。

【請求項３】
前記第１記憶装置は、第１記憶領域及び第２記憶領域を含み、前記第１記憶装置は起動後に外部から見える空間が第１記憶領域であり、前記第１記憶領域は安全管理プログラムを予め記憶し、外部アクセスデータアドレスが第１記憶領域の空間のサイズより大きい場合に任意のデータを返送し、このときに前記第２記憶領域はロック状態として外部から見えなく、前記第２記憶領域は、実際に外部で利用可能な記憶空間であり、アンロック後に見えて利用可能であり、
前記第１記憶装置が検出された時に前記第１記憶装置に予め記憶された安全管理プログラムをロードすることは、
前記第１記憶装置が検出された時に、第１記憶領域に予め記憶された安全管理プログラムをロードことを含み、
前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づいてオペレーティングシステムを動作する前には、前記記憶データ安全動作方法は、さらに、
前記第１記憶装置は、暗号化の身分情報を復号化して検証し、検証が成功した場合に前記第２記憶領域のロックを解除することを含む
ことを特徴とする請求項１に記載の記憶データ安全動作方法。
【請求項４】
前記第２記憶領域のロックを解除した後に、前記記憶データ安全動作方法は、さらに、
前記第１記憶装置が前記第１記憶領域をロックすることを含む
ことを特徴とする請求項３に記載の記憶データ安全動作方法。
【請求項５】
第１記憶装置が検出された時に、第１記憶装置に予め記憶された安全管理プログラムをロードすることは、
電源投入時に第１記憶装置を検出することと、
第１記憶装置の第１記憶領域に記憶されたブートプログラムを読み取ることと、
第１ブートプログラムを動作することと、
第１記憶装置に予め記憶された安全管理プログラムをロードすることと、を含む
ことを特徴とする請求項１に記載の記憶データ安全動作方法。
【請求項６】
前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づいてオペレーティングシステムを動作することは、
前記第１記憶装置で身分情報を復号化し、検証が成功した後に安全管理プログラムを継続して動作させることと、
第２ブートプログラムをロードして動作させることと、
システムデータをロードしてオペレーティングシステムを動作することと、を含む
ことを特徴とする請求項１に記載の記憶データ安全動作方法。
【請求項７】
ホストと、第１記憶装置とを含み、前記第１記憶装置は前記ホストと通信可能に接続され、前記ホストは、第１記憶装置が検出された時に第１記憶装置に予め記憶された安全管理プログラムをロードする、記憶データ安全動作システムであって、
前記ホストは、安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得し、
前記ホストは、暗号化の身分情報を前記第１記憶装置に送信し、
前記第１記憶装置は、身分情報を復号化して検証し、
前記ホストは、前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づいてオペレーティングシステムを動作し、
前記ホストは、安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得することは、
安全管理プログラムを動作して第２記憶装置を検出し、前記第２記憶装置が検出された時

に前記第２記憶装置に予め記憶された暗号化の身分情報を読み取ること、を含み、
前記第２記憶装置は、挿抜可能な記憶装置とする
ことを特徴とする記憶データ安全動作システム。
【請求項８】
前記第１記憶装置は、第１記憶領域及び第２記憶領域を含み、
前記第１記憶領域は、安全管理プログラムを記憶し、前記第１記憶領域は、前記第２記憶領域がアンロックされた後にロック状態とし、
前記第２記憶領域は、システムデータを記憶し、前記第２記憶領域は、身分情報を復号化し、検証が成功する前にロック状態とする
ことを特徴とする請求項７に記載の記憶データ安全動作システム。
【請求項９】
前記ホストに通信可能に接続され、前記ホストにより検出された後に前記ホストから送信された情報取得命令を受信し、暗号化の身分情報を前記ホストに送信する、第２記憶装置を、さらに備える
ことを特徴とする請求項７に記載の記憶データ安全動作システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報技術の分野に関し、具体的には、記憶データ安全動作方法及びシステムに関する。
【背景技術】
【０００２】
データ安全記憶および応用は、徐々に使用者に知られるようになってきたが、暗号化機能付きの安全記憶装置を便利に使用する方法や既存の応用シーンとスムーズとを結合する方法は、暗号化記憶装置で記憶するとのソリューションがユーザに受け入れられるかどうかを決定する要因である。
【０００３】
現在、市場で認証付きの安全暗号化記憶装置は、データが安全暗号化記憶装置の媒体に暗号文で記憶されている。装置は、データをアクセスする前にユーザの身分を認証し、認証成功の後で装置のロックを解除し、データをアクセスすることができるようになる必要がある。認証付きの安全暗号化記憶装置は、ホストユーザの身分をチェックする必要があるので、正当なユーザのみでハードディスクデータをアクセスすることを許可し、ある程度の安全性を有する。一方、認証付きの安全暗号化記憶装置は、内部のデータ暗復号の鍵がユーザの身分鍵によって厳格に保護されることによって、正しいユーザのログインの鍵がないと正しいデータ暗復号の鍵を取得できないので、ユーザのデータの安全を最大限に保証する。
【０００４】
しかしながら、認証付きの安全暗号化記憶装置は、ホスト側でユーザ身分の鍵を入力する必要がある。このような入力インタフェースは、オペレーティングシステムＯＳ上で動作するプログラムで提供されるヒューマンインタフェースに基づいて行われることが多いものであり、ユーザが入力した身分の鍵を、ホストと装置との間の記憶インタフェースを介して記憶装置に取り込む。記憶装置の検証が成功した後に、ホストは記憶装置に記憶されたデータにアクセスすることができる。ロック解除の前に記憶装置に記憶されたデータに正当にアクセスできないため、オペレーティングシステムやロック解除インタフェースを提供するプログラムを、ロック解除が必要で認証付きの安全暗号記憶装置に直接に記憶することができない。即ち、認証付きの安全暗号記憶装置は、データディスクとして機能するだけで、システムディスクとしては機能しない。そのため、オペレーティングシステムやロック解除のインタフェースを提供するプログラムを認証付きの安全暗号記憶装置に記憶することは、ハードディスクに対してロックを解除する必要がある。例えば、認証インタフェース付きのプログラムをＢＩＯＳに記憶し、ＢＩＯＳフェーズで安全暗号化記憶

装置からデータを読み取る前にロックを解除する。そして、システムをロードする。しかしながら、これは、ＢＩＯＳをカスタマイズ化する（ＢＩＯＳの機能拡張）必要があるので、ＢＩＯＳのベンダの違いを考慮してほとんど不可能である。また、ユーザはハードディスクのロックを解除するために身分鍵を手で入力する必要があり、操作感が悪い。

【発明の概要】

【０００５】

本発明の実施例は、上記の問題を改善し、記憶データ安全動作方法及びシステムを提供することを目的とする。

【０００６】

一態様において、本願実施例は、記憶データ安全動作方法を提供し、前記記憶データ安全動作方法は、

第１記憶装置が検出された時に、前記第１記憶装置に予め記憶された安全管理プログラムをロードすることと、

安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得することと、

暗号化の身分情報を前記第１記憶装置に送信することと、

前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づいてオペレーティングシステムを動作することと、を含む。

【０００７】

一態様において、本願実施例は、記憶データ安全動作システムを提供し、

前記ホストは第１記憶装置が検出された時に、第１記憶装置に予め記憶された安全管理プログラムをロードし、

前記ホストは、安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得し、

前記ホストは、暗号化の身分情報を前記第１記憶装置に送信し、

前記第１記憶装置は身分情報を復号化して検証し、

前記ホストは、前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づいてオペレーティングシステムを動作する。

【０００８】

従来技術と比較して、本発明が提供する記憶データ安全動作方法及びシステムは、第１記憶装置が検出された場合に第１記憶装置に予め記憶された安全管理プログラムをロードすることと、安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得することと、暗号化の身分情報を前記第１記憶装置に送信することと、前記第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、最後にシステムデータに基づいてオペレーティングシステムを動作することと、を含む。これにより、安全にオペレーティングシステムを動作するとともに、ＢＩＯＳを拡張する必要がなく、人手で動作する必要がなく、ユーザ体験がよく、安全管理プログラムが第１記憶装置に予め記憶されてホストの記憶空間を節約する。

【０００９】

本発明の上記目的、特徴および利点をより明瞭にするために、以下で好ましい実施例を挙げ、添付の図面と結合して以下に詳細に説明する。

【図面の簡単な説明】

【００１０】

本発明の実施例の目的、技術案及び利点をより明確にするために、以下、本発明の実施例の図面を参照し、本発明の実施例の技術案を明確で完全に説明する。明らかに、説明の実施例は、本発明の一部の実施例であり、全ての実施例ではない。本明細書において一般に説明する添付の図面に示される本発明の実施例の構成要素は、様々な異なる構成で配置および設計されるものである。したがって、添付図面に示される本発明の実施例の以下の詳細な説明は、請求項として本発明の範囲を限定することを意図するものではなく、本発明の選択とする実施例のみを示す。本発明の実施例に基づいて、当業者が発明の進歩性を有する努力をせずに思いつく他のすべての実施例は本発明の保護範囲に含まれている。

【００１１】
【図１】図１は本発明の実施例による記憶データ安全動作システムで相互的な概略図である。
【図２】図２は本発明の実施例によるホストの構成のブロック図である。
【図３】図３は本発明の実施例による記憶データ安全動作装置の機能ユニットのブロック図である。
【図４】図４は本発明の実施例に係るロードユニットの第１実施例のサブモジュールの概略図である。
【図５】図５は本発明の実施例に係るロードユニットの第１実施例のサブモジュールの概略図である。
【図６】図６は本発明の実施例による記憶データ安全動作方法のフローチャートである。
【発明を実施するための形態】
【００１２】
以下、本発明の実施例の図面を参照し、本発明の実施例の技術案を明確で完全に説明する。明らかに、説明の実施例は、本発明の一部の実施例であり、全ての実施例ではない。本明細書において一般に説明する添付の図面に示される本発明の実施例の構成要素は、様々な異なる構成で配置および設計されるものである。したがって、添付図面に示される本発明の実施例の以下の詳細な説明は、請求項として本発明の範囲を限定することを意図するものではなく、本発明の選択とする実施例のみを示す。本発明の実施例に基づいて、当業者が発明の進歩性を有する努力をせずに思いつく他のすべての実施例は本発明の保護範囲に含まれている。
【００１３】
本発明の実施例による記憶データ安全動作方法及びシステムは、記憶データ安全動作方法を提供する。該記憶データ安全動作方法は、ホスト１０１に適用可能である。ホストは、個人用ＰＣであってもよい。このホスト１０１は、スマートフォン、ＰＣ、タブレット、PDA、MID、サーバなどであってもよいが、これらに限定されない。前記ホスト２００のオペレーティングシステムは、Androidシステム、ＩＯＳシステム、Windows phoneシステム、Windowsシステムなどであってもよいが、これに限定されない。ホスト１０１は、第１記憶装置２００、第２記憶装置３００とそれぞれに通信に接続され、記憶データ安全動作システムを構成する。
【００１４】
図２は、前記ホスト１０１のブロック図を示す。前記ホスト１０１は、記憶データ安全動作装置１００、プロセッサ１０２、メモリ１０３、メモリコントローラ１０４、外部インタフェース１０５、表示モジュール１０６を含む。
【００１５】
前記メモリ１０３、前記メモリコントローラ１０４及び前記プロセッサ１０２は、各素子が互いに直接又は間接的に電気的に接続され、データの伝送又は交換を実現する。例えば、これらの要素は、１つまたは複数の通信バスまたは信号線によって互いに電気的に接続されてもよい。前記記憶データ安全動作装置１００は、ソフトウェアまたはファームウェアの形態で前記メモリ１０３に記憶されてまたは前記ホスト１０１のオペレーティングシステム（ＯＳ）内でキュアされて少なくとも１つのソフトウェア機能モジュールを含む。前記プロセッサ１０２は、メモリ１０３に記憶された動作可能なモジュールを動作する。例えば、前記記憶データ安全動作装置１００は、ソフトウェア機能モジュール又はコンピュータプログラムを含む。
【００１６】
ここで、メモリ１０３は、ランダムアクセスメモリ（Random Access Memory、RAM）、リードオンリーメモリ（Read Only Memory、ROM）、プログラマブルリードオンリーメモリ（Programmable Read-Only Memory、PROM）、消去可能リードオンリーメモリ（Erasable Programmable Read-Only Memory、EPROM）、電気的に消去可能リードオンリーメモリ（Electric Erasable Programmable Read-Only

Memory、EEPROM）などであってもよいが、これに限定されない。メモリ１０３は、プログラムを記憶する。前記プロセッサ１０２は、動作命令を受信した後に前記プログラムを動作する。本発明の実施例のいずれかに開示されたフローで定義するホスト１０１が動作する方法は、前記プロセッサ１０２に適用されてもよく、プロセッサ１０２によって実現されてもよい。

【００１７】

プロセッサ１０２は、集積回路チップで信号の処理能力を有する。上述したプロセッサ１０２は、汎用プロセッサであり、Central Processing Unit（CPU）、Network Processor（NP）などを含む。また、デジタル信号プロセッサ（DSP）、専用集積回路（ASIC）、既製のプログラマブルゲートアレイ（FPGA）または他のプログラマブル論理素子、個別ゲートまたはトランジスタ論理素子、個別ハードウェア構成要素であってもよい。本発明の実施例に開示された方法、ステップ及び論理ブロック図を実現または動作することができる。汎用プロセッサは、マイクロプロセッサであってもよく、任意の従来のプロセッサなどであってもよい。

【００１８】

外部インタフェース１０５は、様々な入力/入力装置をプロセッサおよびメモリ１０３に結合する。一実施例において、外部インタフェース１０５、プロセッサ１０２及びメモリコントローラ１０４は、単一のチップに実現されてもよい。他の実施例において、それらはそれぞれに別個のチップによって実現される。

【００１９】

表示モジュール１０６は、前記ホスト１０１とユーザとの間で相互インタフェース（例えば、ユーザ操作インタフェース）を提供し、または画像データをユーザに表示して参照する。例えば、ホスト１０１にインストールされているブラウザがロードしたウェブページの内容を表示する。表示モジュール１０６は、液晶ディスプレイ又はタッチディスプレイであってもよい。タッチディスプレイの場合に、単点及び多点タッチ操作をサポートする静電容量式タッチスクリーン又は抵抗膜式タッチスクリーンなどであってもよい。単点及び多点のタッチ操作をサポートすることは、タッチディスプレイが該タッチディスプレイの１つまたは複数の位置から同時に生じるタッチ操作を検知し、その検知したタッチ操作をプロセッサ１０５によって計算および処理することができる意味である。

【００２０】

図３を参照し、本発明の実施例は、記憶データ安全動作装置１００を提供する。前記記憶データ安全動作装置１００は、ロードユニット３０１と、動作ユニット３０２と、読み取りユニット３０３と、情報送信ユニット３０４とを備える。

【００２１】

ロードユニット３０１は、第１記憶装置２００を検出した時に第１記憶装置２００に予め記憶された安全管理プログラムをロードする。

【００２２】

本実施例において、安全管理プログラムは２つの部分を含み、一部は鍵管理メインプログラムであり、動作される時に第２記憶装置３００に記憶された暗号化のユーザ身分情報を読み取り、ホスト１０１を介して第１記憶装置２００に返送して第１記憶装置２００にロックを解除する。もう一部は、鍵管理プログラムのブートプログラムであり、ホストのＢＩＯＳにロードされて鍵管理プログラムをロードする。

【００２３】

具体的には、図４に示すように、前記ロードユニット３０１は、検出サブモジュール４０１、読み取りサブモジュール４０２、第１動作サブモジュール４０３及び第１ロードサブモジュール４０４を含む。ロードユニット３０１は、ＢＩＯＳで動作するソフトウェア装置であってもよい。

【００２４】

検出サブモジュール４０１は、電源投入時に第１記憶装置２００を検出する。

【００２５】

ここで、第１記憶装置２００は、ハードディスク、又はハードディスクを内蔵したスマート端末（例えば、ハードディスクを内蔵したノートパソコン）としてもよい。前記第１記憶装置２００は、安全管理プログラムを記憶する第１記憶領域３０５と、システムデータを記憶する第２記憶領域３０６と、を含む。システムデータは、オペレーティングシステムデータとユーザデータとを含む。ここで、第１記憶領域３０５は、第１記憶装置２００がロック状態にある時にアクセスされる。第２記憶領域３０６は、第１記憶装置２００がアンロック状態にある時にアクセスされる。なお、第１記憶装置２００の初期状態はロック状態であり、第１記憶装置２００がロック状態にある時には、ホスト１０１が第１記憶領域３０５のみにアクセス可能である。

【００２６】

読み取りサブモジュール４０２は、第１記憶装置２００を検出した際に第１記憶装置２００に記憶されたブートプログラムを読み取る。第１動作サブモジュール４０３は、第１ブートプログラムを動作させる。第１ロードサブモジュール４０４は、第１ブートプログラムの動作後に第１記憶装置２００に予め記憶された安全管理プログラムをロードする。

【００２７】

動作ユニット３０２は、安全管理プログラムを動作して第２記憶装置３００を検出する。

【００２８】

第２記憶装置３００は、挿抜可能な記憶装置とする。例えば、ＵディスクまたはＵシールドであってもよいが、これに限定されない。

【００２９】

読み取りユニット３０３は、第２記憶装置３００を検出した時に第２記憶装置３００に予め記憶された暗号化の身分情報を読み取る。

【００３０】

ユーザ身分の鍵情報が暗号文として第２記憶装置３００に記憶され、暗号文で第２記憶装置３００に送信されるので、ユーザ身分の鍵情報の安全を確保する。本実施例において、ユーザ身分情報は、非対称復号化アルゴリズムの公開鍵と秘密鍵とのペアのうちの秘密鍵を暗号化してユーザ身分の鍵情報を形成して記憶する。また、ユーザ身分情報の鍵は、公開鍵と秘密鍵のうちの公開鍵を交換し、公開鍵で暗号化した後に第２記憶装置３００に送信して記憶させる。これにより、暗号文が固定的なものでなく、送信する毎に異なることを保証でき、より高い安全性を持たせることができる。

【００３１】

情報送信ユニット３０４は、暗号化の身分情報を前記第１記憶装置２００に送信する。

【００３２】

このときに、第１記憶装置２００は暗号化の状態にある身分情報を復号化し、復号化した身分情報と予め記憶している身分情報とが一致するか否かを判断する。一致する場合には、認証成功となる。このときに、第１記憶装置２００はアンロックされる。このときに第１記憶装置２００の第２記憶領域３０６はホスト１０１から直接アクセス可能となる。

【００３３】

前記ロードユニット３０１は、前記第１記憶装置２００で身分情報を復号化し、検証が成功した後にシステムデータをロードする。

【００３４】

第１記憶装置２００のロックが解除されたので、ホスト１０１は、第１記憶装置２００の第２記憶領域３０６のシステムデータに直接にアクセスすることができる。

【００３５】

具体的には、図５に示すように、ロードユニット３０１は、第２動作サブモジュール５０１、第２ロードサブモジュール５０２、第３動作サブモジュール５０３、第３ロードサブモジュール５０４をさらに含む。

【００３６】

第２動作サブモジュール５０１は、前記第１記憶装置２００で身分情報を復号化し、検証が成功した後に安全管理プログラムを継続して動作する。

【００３７】
第２ロードサブモジュール５０２は、安全管理プログラムを動作する際に第２ブートプログラムをロードする。
【００３８】
第３動作サブモジュール５０３は、第２ブートプログラムを動作させる。
【００３９】
第３ロードサブモジュール５０４は、第２ブートプログラムを動作する際にシステムデータをロードする。
【００４０】
前記動作ユニット３０２は、システムデータに基づいてオペレーティングシステムを動作する。
【００４１】
図６を参照し、本発明の実施例は、記憶データ安全動作方法をさらに提供する。本実施例が提供する記憶データ安全動作方法は、その原理及び技術効果が上述した実施例と同様である。従って、説明を簡単にするために、本実施例では一部言及していない点が上述した実施例に対応する内容を参照する。前記記憶データ安全動作方法は、以下のステップを含む。
【００４２】
ステップＳ６０１：第１記憶装置２００が検出された時に第１記憶装置２００に予め記憶された安全管理プログラムをロードする。
【００４３】
前記第１記憶装置２００は、第１記憶領域３０５と第２記憶領域３０６を含み、前記第１記憶装置２００は、起動後に外部から見える空間が第１記憶領域３０５である。前記第１記憶領域３０５は安全管理プログラムを予め記憶する。外部アクセスデータアドレスが第１記憶領域３０５の空間のサイズより大きい場合には、任意のデータを返送する。この時、前記第２記憶領域３０６はロック状態にあり、外部から見えない。前記第２記憶領域３０６は、実際に外部から利用可能な記憶領域であり、ロック解除後に見えて利用も可能となる。
【００４４】
第１記憶装置２００が検出された場合には、第１記憶領域３０５に予め記憶された安全管理プログラムをロードする。具体的には、ステップＳ６０１は、電源投入時に第１記憶装置２００を検出することと、第１記憶装置２００の第１記憶領域３０５に記憶されたブートプログラムを読み取ることと、第１ブートプログラムを動作させることと、第１記憶装置２００に予め記憶された安全管理プログラムをロードすることと、を含む。
【００４５】
ステップＳ６０２：安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得する。
【００４６】
例えば、安全管理プログラムを動作して第２記憶装置３００を検出し、第２記憶装置３００が検出された場合には、前記第２記憶装置３００に予め記憶された暗号化の身分情報を読み取る。また、例えば、安全管理プログラムを動作し、ホストに予め記憶された暗号化の身分情報を読み取る。
【００４７】
ステップＳ６０３：暗号化の身分情報を前記第１記憶装置２００に送信する。
【００４８】
ステップＳ６０４：前記第１記憶装置２００は、暗号化の身分情報を復号化して検証する。検証が成功した場合には、第２記憶領域３０６のロックを解除する。
【００４９】
ステップＳ６０５：前記第１記憶装置２００は、前記第１記憶領域３０５をロックする。
【００５０】

ステップＳ６０６：前記第１記憶装置２００で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに基づくオペレーティングシステムを動作する。

【００５１】

具体的には、ステップＳ６０６は、前記第１記憶装置２００で身分情報を復号化し、検証が成功した後に安全管理プログラムの動作を継続して動作することと、第２ブートプログラムをロードして動作することと、システムデータをロードしてオペレーティングシステムを動作することとを、含む。

【００５２】

図１を参照し、本発明の実施例は、さらに、記憶データ安全動作システムを提供する。前記記憶データ安全動作システムは、ホスト１０１、第１記憶装置２００、第２記憶装置３００を含む。前記第１記憶装置２００、前記第２記憶装置３００がそれぞれに前記ホスト１０１と通信可能に接続されている。ホスト１０１は、第１記憶装置２００が検出された時に第１記憶装置２００に予め記憶された安全管理プログラムをロードする。

【００５３】

ホスト１０１は、安全管理プログラムを動作し、予め記憶された暗号化の身分情報を取得する。

【００５４】

前記ホスト１０１は、暗号化の身分情報を前記第１記憶装置２００に送信する。

【００５５】

前記第１記憶装置２００は、身分情報を復号化して検証する。

【００５６】

前記ホスト１０１は、前記第１記憶装置２００で身分情報を復号化し、検証が成功した後にシステムデータをロードし、システムデータに従ってオペレーティングシステムを動作する。

【００５７】

ここで、前記第１記憶装置２００は、挿抜可能な記憶装置としてもよい。前記第１記憶装置２００は、安全管理プログラムを記憶する第１記憶領域３０５を含む。ここで、第１記憶領域３０５は、第２記憶領域３０６のロックを解除した後にロック状態にある。第２記憶領域３０６は、身分情報を復号化して検証が成功する前にロック状態にある。第１記憶装置２００は、ハードディスク又はハードディスクを内蔵したスマート端末を採用する。第１記憶装置２００（即ち、第２記憶領域３０６）がロック状態（即ち、身分検証が成功する前）の場合には、ホスト１０１がアクセスする記憶領域は第１記憶領域３０５である。第１記憶領域３０５のサイズは実際に記憶されているデータ量に応じて予め置き、ホスト１０１のアクセスが第１記憶装置２００を超える場合に、そのままオールゼロでデータを返す。第１記憶装置２００がアンロック状態（第２記憶領域３０６がアンロック状態）である場合（即ち、認証成功後）には、第２記憶領域３０６にアクセスできる。

【００５８】

以上をまとめると、本発明が提供する記憶データ安全動作方法及びシステムは、第２記憶装置が検出された場合に前記第２記憶装置に予め記憶された暗号化の身分情報を取得することと、暗号化の身分情報を第１記憶装置に送信することと、第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータをロードし、最後にシステムデータに基づいてオペレーティングシステムを動作することと、を含む。これにより、安全にオペレーティングシステムを動作するとともに、ＢＩＯＳを拡張する必要がなく、人手で動作する必要がなく、ユーザ体験がよく、安全管理プログラムが第１記憶装置に予め記憶されてホストの記憶空間を節約する。

【００５９】

本明細書で提供されるいくつかの実施例において、記載の装置および方法は、他の方法でも実現されることが理解されている。上述の装置実施例は、単なる例示である。例えば、図面のフローチャート及びブロック図は、本発明の様々な実施例による装置、方法、及

びコンピュータプログラム製品で実現可能なアーキテクチャ、機能及び動作を示す。この点に関して、フローチャート又はブロック図における各ブロックは、１つのモジュール、セグメント、又はコードの一部を表す。該モジュール、セグメント、又はコードは、規定の論理機能を実施する１つ又は複数の動作可能な命令を含む。いくつかの代りとする実装形態において、ブロックに記された機能は、図に記された順序とは異なる順序で奏してもよい。例えば、２つの連続するブロックは、実際に並列に動作されてもよいが、その機能に応じて逆順に動作されてもよい。なお、ブロック図及び/又はフローチャート図における各ブロック、並びにブロック図及び/又はフローチャート図のブロックの組み合わせは、規定の機能又は操作を動作する専用ハードウェアベースのシステムで実現されてもよく、又は専用ハードウェアとコンピュータ命令との組み合わせで実現されてもよい。

【００６０】

また、本発明の各実施例における各機能ブロックは、１つに統合されて独立した部分を形成してもよく、各ブロックが個別に存在してもよく、２つ以上のブロックが統合されて独立した部分を形成してもよい。

【００６１】

上記機能はソフトウェア機能モジュールの形態で実現され、独立した製品として販売または使用される場合には、コンピュータ読み取り可能な記憶媒体に記憶されてもよい。このような理解に基づいて、本発明の技術案は、本質的にあるいは従来技術に貢献する部分またはその一部を、ソフトウェア製品の形態で具体化する。該ソフトウェア製品は記憶媒体に記憶され、コンピュータ装置（パーソナルコンピュータ、サーバ、またはネットワーク装置などとすることができる）に、本発明の各実施例で説明された方法のステップの全部または一部を動作させる複数の命令を含む。また、上記記憶媒体としては、Ｕディスク、ポータブルハードディスク、ＲＯＭ（Read-Only Memory）、ＲＡＭ（Random Access Memory）、磁気ディスクまたは光ディスクなど種々プログラムコードが記憶可能な媒体含む。なお、本明細書では、第１、第２などの関係用語は、単に一の実体または操作と他の実体または操作とを区別するために使用されたものであり、必ずしも実体または操作の間で実際にそのような関係または順序が存在することを要求または暗示するものではない。さらに、「備える」、「含む」、またはそれらの任意の他の変形例は、非排他的な包含をカバーするように意図するものである。したがって、一連の要素を含むプロセス、方法、品目、または装置は、それらの要素だけでなく、明示的に列挙されていない他の要素も含む。または、そのようなプロセス、方法、品目、または装置に固有の要素も含む。これ以上に限定がないと前提にし、「……を含む」という表現によって定義される要素は、その要素に他の前記要素を含むプロセス、方法、物品、又は装置が存在することを除外しない。

【００６２】

以上の説明は、本発明の好ましい実施例に過ぎず、本発明を限定するものではない。当業者は種々の変更及び変形が可能である。本発明の主旨及び原理を逸脱しない範囲において、任意の修正、均等取り替え、改良等が行われるものは、本発明の保護範囲に含まれる。なお、以下の図面において同様の符号および文字は同様の項目を表しており、一度に定義された項目は以降の図面でさらに定義して説明される必要がない。

【００６３】

以上の説明は、本発明の具体的な実施例だけである。本発明の保護範囲は、これに限定されない。当業者は、本発明の技術範囲において変更又は置換を容易に想到するものが本発明の保護範囲に含まれる。したがって、本発明の保護範囲は、記載の請求項の保護範囲を基準として記載される。

【００６４】

なお、本明細書では、第１、第２などの関係用語は、単に一の実体または操作と他の実体または操作とを区別するために使用されたものであり、必ずしも実体または操作の間で実際にそのような関係または順序が存在することを要求または暗示するものではない。さらに、「備える」、「含む」、またはそれらの任意の他の変形例は、非排他的な包含をカ

バーするように意図するものである。したがって、一連の要素を含むプロセス、方法、品目、または装置は、それらの要素だけでなく、明示的に列挙されていない他の要素も含む。または、そのようなプロセス、方法、品目、または装置に固有の要素も含む。これ以上に限定がないと前提にし、「……を含む」という表現によって定義される要素は、その要素に他の前記要素を含むプロセス、方法、物品、又は装置が存在することを除外しない。

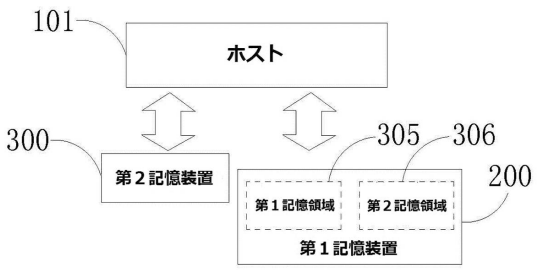
【符号の説明】

【００６５】

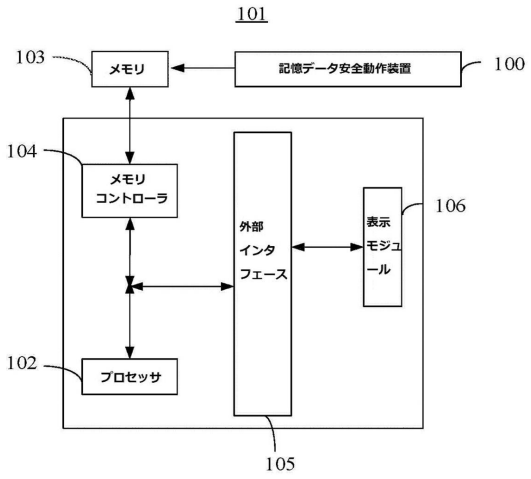
１００　記憶データ安全動作装置；２００　第１記憶装置；
３００　第２記憶装置；１０１　ホスト；１０２　プロセッサ；
１０３　メモリ；１０４　メモリコントローラ；１０５　外部インタフェース；
１０６　表示モジュール；３０１　ロードユニット；３０２　動作ユニット；
３０３　読み取りユニット；３０４　情報送信ユニット；
３０５　第１記憶領域；３０６　第２記憶領域；４０１　検出サブモジュール；
４０２　読み取りサブモジュール；４０３　第１動作サブモジュール；
４０４　第１ロードサブモジュール；５０１　第２動作サブモジュール；
５０２　第２ロードサブモジュール；５０３　第３動作サブモジュール；
５０４　第３ロードサブモジュール。

【図面】

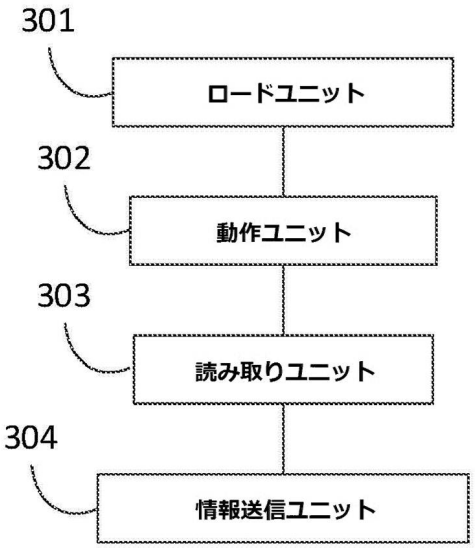
【図１】


101
ホスト
300
第２記憶装置
305
306
200
第１記憶領域
第２記憶領域
第１記憶装置

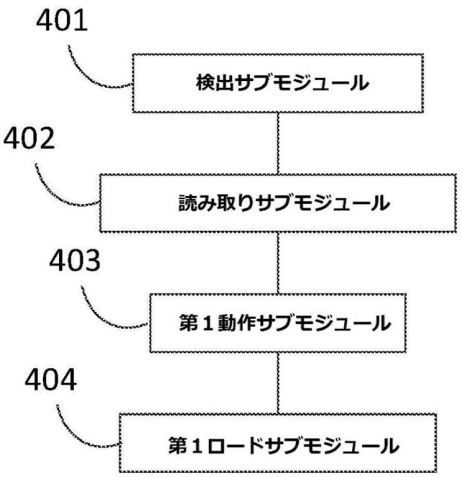
【図２】


101
103
メモリ
記憶データ安全動作装置
100
104
メモリ
コントローラ
外部
インタ
フェース
表示
モジュール
106
102
プロセッサ
105

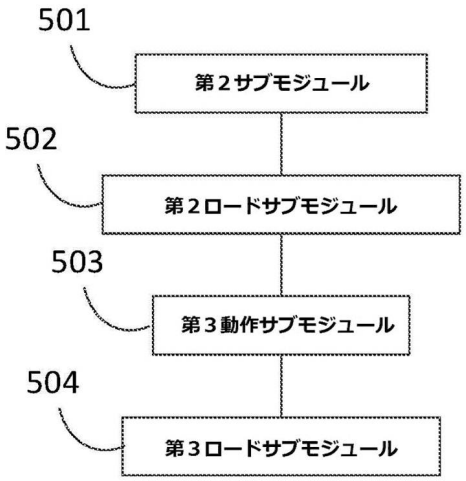
【図３】


301
ロードユニット
302
動作ユニット
303
読み取りユニット
304
情報送信ユニット

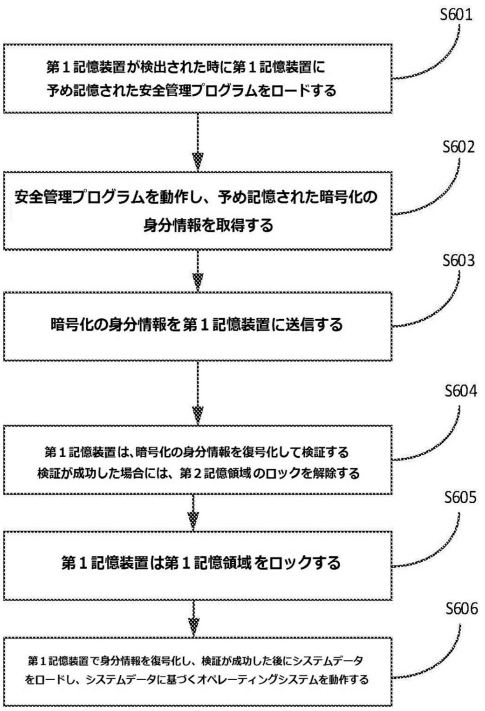
【図４】


401
検出サブモジュール
402
読み取りサブモジュール
403
第１動作サブモジュール
404
第１ロードサブモジュール

【図５】


501
第２サブモジュール
502
第２ロードサブモジュール
503
第３動作サブモジュール
504
第３ロードサブモジュール

【図６】


S601
第１記憶装置が検出された時に第１記憶装置に
予め記憶された安全管理プログラムをロードする
S602
安全管理プログラムを動作し、予め記憶された暗号化の
身分情報を取得する
S603
暗号化の身分情報を第１記憶装置に送信する
S604
第１記憶装置は、暗号化の身分情報を復号化して検証する
検証が成功した場合には、第２記憶領域のロックを解除する
S605
第１記憶装置は第１記憶領域をロックする
S606
第１記憶装置で身分情報を復号化し、検証が成功した後にシステムデータ
をロードし、システムデータに基づくオペレーティングシステムを動作する

フロントページの続き

審査官　小林 秀和
(56)参考文献　特開２００９－０７６０４５（ＪＰ，Ａ）
特開２００９－０４３０３６（ＪＰ，Ａ）
国際公開第２００９／０９０７３４（WO，Ａ１）
特開２０１６－１６３１７３（ＪＰ，Ａ）
特開２０１１－２４８４７４（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５７