(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5355351号
(P5355351)
(45)発行日　平成25年11月27日(2013.11.27)　(24)登録日　平成25年9月6日(2013.9.6)

(51)Int.Cl.　　F I
G06F 21/56 (2013.01)　　G06F 21/00 156A
G06F 21/10 (2013.01)　　G06F 21/22

請求項の数 7　(全 12 頁)

(21)出願番号　特願2009-254921 (P2009-254921)
(22)出願日　平成21年11月6日 (2009.11.6)
(65)公開番号　特開2011-100329 (P2011-100329A)
(43)公開日　平成23年5月19日 (2011.5.19)
審査請求日　平成24年8月2日 (2012.8.2)

(73)特許権者　000233055
株式会社日立ソリューションズ
東京都品川区東品川四丁目１２番７号
(74)代理人　100088720
弁理士　小川　眞一
(72)発明者　鮫島　吉喜
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

審査官　脇岡　剛

最終頁に続く

(54)【発明の名称】コンピュータ

(57)【特許請求の範囲】
【請求項１】
暗号化データを内部にある鍵で復号し、その復号したデータに含まれる条件値と内部レジスタの値が一致したときに復号結果を出力する暗号ハードウェアモジュールと、アクセスするプログラムが正規のプログラムと認証した後にアクセス可能になる第１の領域と認証なしにアクセス可能な第２の領域とに分かれたハードディスクを搭載したコンピュータにおいて、
コンピュータ起動時のプログラムが、上記ハードディスクの認証なしにアクセス可能な第２の領域のハッシュ値を計算し、前記暗号ハードウェアモジュールの内部レジスタに格納し、第２の領域のプログラムをメモリにロードして処理を引き渡し、処理を引き渡された第２の領域にあったプログラムがハードディスクに対して認証処理を行い、正規プログラムであるという認証を得た後に前記第１の領域にアクセスし、当該第１の領域にあるプログラムをメモリにロードすることを特徴とするコンピュータ。
【請求項２】
前記第２の領域にあったプログラムが、プログラム中に含まれるパスワードをハードディスクに送ることによってハードディスクに対する認証処理を行うことを特徴とする請求項１に記載のコンピュータ。
【請求項３】
前記第２の領域にあったプログラムが、当該プログラム中に含まれる暗号データを前記暗号ハードウェアモジュールに送り、当該暗号ハードウェアモジュールが内部にある鍵で

前記暗号データを復号し、復号した条件値と内部レジスタに格納されている第２の領域のハッシュ値と比較し、一致した場合に復号データを出力し、その復号データを前記第２の領域にあったプログラムが受取り、復号データ中に含まれているパスワードをハードディスクに送ることによってハードディスクに対する認証処理を行うことを特徴とする請求項１に記載のコンピュータ。

【請求項４】

前記第２の領域にあったプログラムが、当該プログラム中に含まれる暗号データを前記暗号ハードウェアモジュールに送り、当該暗号ハードウェアモジュールが内部にある鍵で前記暗号データを復号し、復号した条件値と内部レジスタに格納されている第２の領域のハッシュ値とを比較し、一致した場合に復号データに含まれる鍵を内部に保管し、この鍵のハンドルを出力し、前記第２の領域にあったプログラムが前記ハンドルを受け取り、このハンドルを元に暗号ハードウェアモジュール内にある鍵を使ってハードディスクに対する認証処理を行うことを特徴とする請求項１に記載のコンピュータ。

【請求項５】

前記第２の領域にあったプログラムが、ハードディスクに対する認証後に前記第１の領域にあるプログラムのハッシュ値を計算し、前記暗号ハードウェアモジュールの内部レジスタに格納した後、当該該プログラムをメモリにロードして処理を引き渡し、処理を引き渡されたプログラムが、引き続き処理を行うことを特徴とする請求項１に記載のコンピュータ。

【請求項６】

前記処理を引き渡されたプログラムが、前記第１の領域のウィルス検査を行うことを特徴とする請求項５に記載のコンピュータ。

【請求項７】

前記処理を引き渡されたプログラムが、起動監視サーバに起動可否を問い合わせ、サーバにアクセスできない場合やアクセスできても予め設定された利用環境条件と一致しない場合には、エラーを表示し、その後の処理を停止させることを特徴とする請求項５に記載のコンピュータ。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、Trusted Computing Group (TCG)のStorage WGの標準に基づいたハードディスクを搭載したパーソナルコンピュータ（以下、ＰＣ）のウィルス検知と利用制限に関するものである。

【０００２】

コンピュータウィルスの一種にMaster Boot Recode (MBR)に感染するタイプがある。

ＭＢＲはコンピュータの起動時に処理されるプログラムであり、ＯＳも既存のウィルス対策プログラムも起動しておらず、一般にウィルス検知が困難である。解決方法の１つとして、特許文献１にあるようなウィルス駆除方法がある。

一方、ＰＣでのセキュリティを実現するためのハードウェアとして、セキュリティ関連の業界標準を定めるTrusted Computing Group (TCG)が定める非特許文献１に挙げるような暗号化を行うセキュリティチップTrusted Platform Module (TPM)の業界標準や非特許文献２にあげるような暗号化ディスクの業界標準がある。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開平１１-０８５５０３号公報

【非特許文献】

【０００４】

【非特許文献１】Trusted Computing Group, TCG Specification, Architecture Overview, Specification, Revision 1.4, 2nd August 2007,p6-p19

【０００５】
【非特許文献２】Trusted Computing Group, TCG Storage Architecture, Core Specification, Specification Version 1.0, Revision 0.9, May 24, 2007, p71-p77
【発明の概要】
【発明が解決しようとする課題】
【０００６】
上記特許文献１に開示された技術にあってはゲートやＲＯＭなどを含む特別なハードウェアを用いる必要があり、導入やコストに課題が残る。またウィルス検知の方法として、ディスク装置にあるウィルスチェックプログラムを利用するとあるが、ウィルスの攻撃方法によっては、本プログラムを破壊したり起動を妨害したりすることも考えられるので、必ずしも有効とはいえない。
また、上記非特許文献１や２に開示された技術にあっては、暗号化ディスクを用いることや特別なハードウェアであるセキュリティチップを用いてプログラムの処理を引き継ぐことが記載されているが、ＭＢＲに感染したウィルスをどのようにして検出するかは具体的に記載されていない。
【０００７】
本発明の目的は、ＯＳ（オペレーティングシステム）が起動する前にＭＢＲなどのシステム領域に感染しているウィルスを検出することができるコンピュータを提供することにある。
また、ウィルスの検出と共に予め設定した環境条件以外の環境でのコンピュータの使用を制限（あるいは禁止）することができるコンピュータを提供することにある。
【課題を解決するための手段】
【０００８】
上記目的を達成するために、本発明に係るコンピュータは、ＴＣＧが標準化しているＴＰＭと呼ばれるセキュリティチップや暗号化ハードディスクを利用し、特別なハードウェアなしにＭＢＲやＯＳ、メモリなどのシステム領域に感染するウィルスをＰＣ起動時に検知する。
具体的には、暗号化データを内部にある鍵で復号し、その復号したデータに含まれる条件値と内部レジスタの値が一致したときに復号結果を出力する暗号ハードウェアモジュールと、アクセスするプログラムが正規のプログラムと認証した後にアクセス可能になる第１の領域と認証なしにアクセス可能な第２の領域とに分かれたハードディスクを搭載したコンピュータにおいて、
コンピュータ起動時のプログラムが、上記ハードディスクの認証なしにアクセス可能な第２の領域のハッシュ値を計算し、前記暗号ハードウェアモジュールの内部レジスタに格納し、第２の領域のプログラムをメモリにロードして処理を引き渡し、処理を引き渡された第２の領域にあったプログラムがハードディスクに対して認証処理を行い、正規プログラムであるという認証を得た後に前記第１の領域にアクセスし、当該第１の領域にあるプログラムをメモリにロードすることを特徴とする。
また、前記第２の領域にあったプログラムが、プログラム中に含まれるパスワードをハードディスクに送ることによってハードディスクに対する認証処理を行うことを特徴とする。
また、前記第２の領域にあったプログラムが、当該プログラム中に含まれる暗号データを前記暗号ハードウェアモジュールに送り、当該暗号ハードウェアモジュールが内部にある鍵で前記暗号データを復号し、復号した条件値と内部レジスタに格納されている第２の領域のハッシュ値と比較し、一致した場合に復号データを出力し、その復号データを前記第２の領域にあったプログラムが受取り、復号データ中に含まれているパスワードをハードディスクに送ることによってハードディスクに対する認証処理を行うことを特徴とする。
また、前記第２の領域にあったプログラムが、当該プログラム中に含まれる暗号データを前記暗号ハードウェアモジュールに送り、当該暗号ハードウェアモジュールが内部にあ

る鍵で前記暗号データを復号し、復号した条件値と内部レジスタに格納されている第２の領域のハッシュ値とを比較し、一致した場合に復号データに含まれる鍵を内部に保管し、この鍵のハンドルを出力し、前記第２の領域にあったプログラムが前記ハンドルを受け取り、このハンドルを元に暗号ハードウェアモジュール内にある鍵を使ってハードディスクに対する認証処理を行うことを特徴とする。

また、前記第２の領域にあったプログラムが、ハードディスクに対する認証後に前記第１の領域にあるプログラムのハッシュ値を計算し、前記暗号ハードウェアモジュールの内部レジスタに格納した後、当該該プログラムをメモリにロードして処理を引き渡し、処理を引き渡されたプログラムが、引き続き処理を行うことを特徴とする。

また、前記処理を引き渡されたプログラムが、前記第１の領域のウィルス検査を行うことを特徴とする。

また、前記処理を引き渡されたプログラムが、起動監視サーバに起動可否を問い合わせ、サーバにアクセスできない場合やアクセスできても否認された場合には、エラーを表示し、その後の処理を停止させることを特徴とする。

【発明の効果】

【０００９】

ＰＣ起動後、ＯＳが起動される前に、ＢＩＯＳによってハードディスクに対する認証なしにアクセス可能な領域であるShadow MBRにあるプログラムが起動され、本プログラムが改ざんされていないと検査した後に、ハードディスクのウィルス検索を行うため、ＯＳ起動前にＭＢＲ等のシステム領域がウィルスに感染していたとしてもＯＳ起動前に確実にこれを検出し対策を実行することができる。

また、ハードディスクに対する認証を行えば、特定のＴＰＭでしか認証できないことになり、ハードディスクを別のＰＣに取り付けて起動しようとしても認証が失敗し、起動もできなくなり、ディスクにアクセスできない。

さらに、データを復号する際にＴＰＭの内部レジスタに記録されたShadow MBRのハッシュ値が正しいか否か検査するために、改竄されたShadow MBRではハードディスクに対する認証ができず、PC起動ができない。

さらに、ウィルス検査とは別に、利用環境条件を設定し、予め設定された利用環境条件と一致しない場合には起動制限を加えることで、時刻や回数、位置などでＰＣの起動を制限することができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施の形態を示す全体構成図である。

【図２】本発明によるＰＣの起動後の動作を説明する説明図である。

【図３】ＰＣ起動時のＢＩＯＳからＭＢＲまでの処理を示すフローチャートである。

【図４】ＴＰＭでパスワードを復号してハードディスクへの認証する場合の処理を示すフローチャートである。

【図５】ＴＰＭの公開鍵暗号機能を利用してハードディスクへの認証する場合の処理を示すフローチャートである。

【図６】ＰＣ起動制限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】

【００１１】

以下、図示する実施の形態に基づいて本発明を詳細に説明する。

図１は、本発明を適用したＰＣの実施の形態を示す全体構成図である。

図１において、１０１は、ＰＣのＣＰＵである。１０２は、ＴＰＭである。通常、ＣＰＵと同じマザーボード上にあり、ＣＰＵやＰＣと一体と看做される。１０３は、メモリである。ＣＰＵ１０１で実行されるプログラムは、メモリ１０３にロードされて、実行される。１０４は、ＢＩＯＳのプログラムである。実体はＲＯＭ上に記録されており、ＲＡＭ（メモリ）１０３にロードされることなく、直接実行される。１０５は、ハードディスクである。本ハードディスクは非特許文献２に準拠しており、起動時にはＳｈａｄｏｗ　Ｍ

ＢＲを読み込むことしかできない。認証に成功すれば、Ｓｈａｄｏｗ　ＭＢＲにアクセス可能なモードに移行したり、ＭＢＲを含むハードディスクにアクセス可能なモードに移行できたりする。

１０８はハードディスク１０５上の認証後の０番地にあるＭＢＲである。通常ＭＢＲにはブートストラップコードやパーティションテーブルが保存されている。

１０９はハードディスク１０５上の認証前、起動直後の０番地にあるＳｈａｄｏｗ　ＭＢＲである。ここに本発明の中心となる処理プログラムが含まれている。

【００１２】

まず、実施の形態の動作を説明する前に、PCの起動、ＴＰＧが標準化しているＴＰＭ、Ｓｈａｄｏｗ　ＭＢＲの概要を説明する。

PC起動の手順は、おおよそ以下の通りである。

電源がＯＮになると、ＢＩＯＳ（Basic I/O system）がハードウェアをテスト、初期化し、ＭＢＲにあるプログラムをメモリ（ＲＡＭ）にロードし、処理を引き継ぐ。処理を引き継いだプログラムはパーティションテーブルを探し、指定されたパーティションにあるブートセクタをメモリにロードし、処理を引き継ぐ。このブートセクタにあるプログラムはＯＳローダをロードし、処理を引き継ぐ。ＯＳローダがＯＳをメモリにロードし、ＯＳを起動する。

【００１３】

以上のように、PC起動時には、ＢＩＯＳ、ＭＢＲのプログラム、パーティションにあるプログラム、ＯＳローダ、ＯＳと、次々にプログラムがメモリにロードされ、制御が渡されていく。ＰＣ上のプログラムの信頼を確保するため、プログラムが次に制御を渡すプログラムのハッシュ値を計算、この結果をＴＰＭにあるレジスタに記録して、制御を渡すように、ＴＣＧは規定している。この方法によれば、最初のＢＩＯＳにあるプログラムが信頼できれば、ＯＳやアプリケーションも改竄のない信頼できるプログラムであることを確認できる。

【００１４】

非特許文献２に記載されているセキュアなハードディスクのＳｈａｄｏｗ　ＭＢＲについて説明する。

Ｓｈａｄｏｗ　ＭＢＲでは、ＰＣ起動時の初期状態にあるハードディスクのＭＢＲと従来の意味でのＭＢＲが異なっている。従来までのセキュアなハードディスクないしは暗号化ハードディスクは、PC起動にパスワード入力が必要であった。すなわちPC起動時にハードディスクにアクセスする認証用のパスワードが必要であり、利用者が入力していた。ハードディスク自体は暗号化されており、ハードディスクドライブに対する認証に成功しなければ、MBRを含めてディスクにアクセスできなかった。

一方、利用者認証方法としては、パスワードのほかに指紋他の生体認証を使った方法や暗号トークンを用いた方法が普及し始めており、ハードディスクに対する認証にも同様の方法が求められるようになると予想される。しかしながら、パスワード認証と比較して、生体認証や暗号トークンを使った認証は、処理が複雑でプログラムサイズが大きい。ＰＣ起動概要に示したとおり、ハードディスクにアクセスする前の処理はＢＩＯＳが行っているが、ＢＩＯＳは複雑で大きな処理を行うにはプログラムのサイズの制限がある。

ＴＣＧの新規格である非特許文献２では、ＰＣ起動時のハードディスクが初期状態にある場合には、従来のＭＢＲの位置には、サイズの大きいＳｈａｄｏｗ　ＭＢＲがあり、ハードディスクへの認証に成功して初めて本来のＭＢＲにアクセスできるようになる。Ｓｈａｄｏｗ　ＭＢＲに生体認証や暗号トークンの認証プログラムを格納しておき、ＢＩＯＳから呼び出されて認証処理を実行、認証に成功した後に、本来のＭＢＲにアクセス可能になり、従来通りの起動が可能となる。

【００１５】

本発明は、上記の二つのＴＣＧの技術を用いて、ＰＣ起動時に安全にウィルス検知を行う。すなわち、ＢＩＯＳがＳｈａｄｏｗ　ＭＢＲのハッシュ値を計算し、ＴＰＭに格納し、Ｓｈａｄｏｗ　ＭＢＲ上のプログラムをメモリにロードして処理を渡す。Ｓｈａｄｏｗ

ＭＢＲのプログラムはハードディスクへの認証処理を行い、本来のＭＢＲにアクセス可能となった時点で、ＭＢＲを含めてウィルスの検索を行い、ウィルスが検知できなければ、従来どおりにＭＢＲにあるプログラムをメモリにロード、処理を引き継ぐ。

【００１６】

Ｓｈａｄｏｗ　ＭＢＲにあるプログラムがハードディスクに対して行う認証処理の方法は複数ある。

第１の認証方法は、単純にパスワードがプログラム中に含まれており、これをハードディスクに送って認証する方法である。ハードディスクは、パスワードが正しければ、正しいＰＣないしはＰＣ上のプログラムがアクセスしていると判断、本来のＭＢＲを含めハードディスクにアクセスできるモードに移行する。

【００１７】

第２の認証方法は、ＴＰＭのＴＰＭ＿Ｕｎｓｅａｌコマンドを使って暗号化されているパスワードをＴＰＭで復号して、このパスワードを用いる方法である。この復号の際には、ＢＩＯＳが計算し、ＴＰＭに格納したＳｈａｄｏｗ　ＭＢＲのハッシュ値が正しいかどうかをＴＰＭが検査するため、改竄されたＳｈａｄｏｗ　ＭＢＲでは復号できず、引いてはハードディスに対する認証もできない。ハッシュ値が正しいか否かは、ＴＰＭ＿Ｓｅａｌコマンドでパスワードを暗号化する際に復号の条件となるＰＣＲの状態を定めることができる。

【００１８】

第３の認証方法は、ＴＰＭや認証トークンにある署名機能を利用した公開鍵暗号ベースの方法である。署名に利用する鍵はＴＰＭ＿ＣｒｅａｔｅＷｒａｐＫｅｙコマンドを使って予め暗号化してある。Ｓｈａｄｏｗ　ＭＢＲは、ＴＰＭ＿ＬｏａｄＫｅｙ２コマンドを使って本データをＴＰＭ内で復号し、この鍵を使ってＴＰＭが生成した署名をハードディスクへの認証に利用する。本コマンドも先のＴＰＭ＿Ｕｎｓｅａｌと同様、ＴＰＭがＳｈａｄｏｗ　ＭＢＲのハッシュ値が正しいか否か、すなわちＳｈａｄｏｗ　ＭＢＲに改竄がないか確認したうえで復号する。

【００１９】

ウィルス検索の方法にも複数ある。

第１にＳｈａｄｏｗ　ＭＢＲがネットワーク機能を持ち、ＰＣ外部にあるウィルスパターンを参照しつつ、ハードディスクにウィルスがないか検索する方法である。

第２にハードディスクのうちシステム部分に当たる部分のハッシュ値を計算、Ｓｈａｄｏｗ　ＭＢＲがもつハッシュ値ないしはネットワーク経由でＰＣ外部にあるハッシュ値と比較、同じであれば改竄がなくウィルスに感染していないと看做す方法である。

第３に最新のウィルスを含まないシステムのイメージをネットワークからダウンロードしてハードディスクにコピーする方法である。

【００２０】

Ｓｈａｄｏｗ　ＭＢＲを使えば、ウィルスないしは改竄検知の他に、Ｓｈａｄｏｗ　ＭＢＲが社内のネットワーク上の特定のサーバにアクセスできるか否かテストし、アクセスできない場合にはＰＣが社外に持ち出されていると判断し、ＰＣ起動処理を停止することで、社外でのＰＣ利用を防止できる。他にも、Ｓｈａｄｏｗ　ＭＢＲが特定サーバにＰＣ起動の可否を問い合わせる、または時刻サーバに問い合わせて自身に記録されている起動許可時間とつき合わせて起動許可時間外ならＰＣ起動を停止することもできる。他にＰＣ起動回数をＳｈａｄｏｗ　ＭＢＲに記録しておき起動制限をかけることもできる。

【００２１】

図２は、本発明によるコンピュータの動作の概要を示す説明図である。

まず、ハードディスク１０５の認証後にアクセス可能に成る第１の領域にはＯＳのブート処理を行うＭＢＲ１０８が記憶されている。また、ハードディスク１０５の認証なしにアクセス可能な第２の領域にはハードディスクの認証処理およびウィルス検出を行うＳｈａｄｏｗ　ＭＢＲ１０９が記憶されている。

Ｓｈａｄｏｗ　ＭＢＲ１０９は、ＯＳの起動前で、かつハードディスクの認証前に、Ｂ

ＩＯＳ１０４によって、制御スイッチ１１１及び１１０を経由して起動される。起動されたＳｈａｄｏｗ　ＭＢＲ１０９は、ハードディスク認証用のパスワードやＳｈａｄｏｗ　ＭＢＲ１０９のハッシュ値などの条件値を含む暗号データ（ＴＰＭ１０２のＴＰＭ＿Ｓｅａｌコマンドを使って暗号化されている）をＴＰＭ１０２に送る。

ＴＰＭ１０２の内部レジスタには、ＢＩＯＳ１０４によって計算されたＳｈａｄｏｗ　ＭＢＲ１０９のハッシュ値が条件値として予め格納されている。

そこで、Ｓｈａｄｏｗ　ＭＢＲ１０９から暗号化データが送られてくると、ＴＰＭ１０２はその暗号化データを内部鍵で復号する。そして、復号した条件値と内部レジスタに格納された条件値とを比較し、一致した場合には、復号したパスワードをＳｈａｄｏｗ　ＭＢＲ１０９に返す。すなわち、Ｓｈａｄｏｗ　ＭＢＲ１０９が改ざんされていなければ、ハッシュ値は一致する筈であるから、復号したパスワードをＳｈａｄｏｗ　ＭＢＲ１０９に返す。

【００２２】

復号したパスワードを受け取ったＳｈａｄｏｗ　ＭＢＲ１０９は、そのパスワードをハードディスク１０５に送る。ハードディスク１０５は自身に設定されているパスワードと一致する場合には、正規のプログラムからのアクセスであると看做し、第１の領域に記憶されているＭＢＲ１０８へのアクセスが可能な状態になり、制御スイッチ１１０が切り替わる。

ＭＢＲ１０８へ処理が移ると、ＯＳのブート処理が実行され、更に制御スイッチ１１１が切り替わってＯＳがＲＡＭ１０３にロードされる。

【００２３】

図３は、ＰＣ起動後のウィルス検索処理の概要を示す。

ステップ３１０において、ＣＰＵテスト後に起動されるＢＩＯＳ１０４のプログラムが起動される。起動されると、ハードウェアのテストや初期化を行い、問題なければ、ハードディスク１０５上にあるＳｈａｄｏｗ　ＭＢＲ１０９全体のハッシュ値を計算、ＴＰＭ１０２の内部レジスタに結果を格納し、Ｓｈａｄｏｗ　ＭＢＲ上のプログラムをメモリ１０３に格納し、制御を渡す。

この処理は起動直後の処理であり、ハードディスク１０５の０番地はＳｈａｄｏｗ　ＭＢＲ１０９である。ハードディスク１０５への認証が成功すれば、０番地は従来のＭＢＲ１０８になる。

なお、ＴＰＭ１０２はハッシュ値をＴＰＭのＰｌａｔｆｏｒｍ　Ｃｒｅｄｅｎｔｉａｌ　Ｒｅｇｉｓｔｅｒ　（ＰＣＲ）というレジスタに格納する。本レジスタは複数あり、システムによって使い方は異なるが、本発明ではＳｈａｄｏｗ　ＭＢＲのハッシュ値のにのみ着目しているので、ＰＣＲは一つと仮定して説明するが、これは本発明の請求範囲を狭めるものではない。

【００２４】

ステップ３２０において、ハードディスク１０５に対する認証処理を行う。認証処理の方法は複数あり、後述する。なお、認証処理に失敗すれば、その旨を利用者に通知、処理を止める。

ステップ３３０においては、ハードディスク１０５に対する認証処理は成功しており、Ｓｈａｄｏｗ　ＭＢＲ１０９を除き、ＭＢＲ１０８を含めてハードディスク１０５全体にアクセスできる。ＲＡＭ１０３上のＳｈａｄｏｗ　ＭＢＲにあったプログラムは、ハードディスクに対するウィルス検索を行う。ウィルスが見つかれば、その旨を利用者に通知、処理を止める。

ステップ３４０においては、ハードディスク１０５の０番地にあるＭＢＲ１０８のブートストラップコードをメモリ１０３にロード、制御を渡す。以降の処理は、通常のＰＣ起動と同じであり、本発明の対象外である。

【００２５】

ここで、ステップ３２０にて行うハードディスク１０５に対する認証処理を述べる。

第１の認証方法として、単純なパスワード認証がある。これは、Shadow MBR１０９中に

あるパスワードをハードディスクに送信することで認証するものである。本方法には、ハードディスクをブートディスクとしないPCに接続すれば、Shadow MBR１０９を読み込むことができ、プログラムを解析すればパスワードが盗まれてしまう危険性があるので推奨できない。

以下の第２と第３の認証方法は、これを解決するものであり、特定のＴＰＭ１０２が搭載された特定のＰＣだけで可能な方法である。すなわち他のＰＣに接続したとしてもＴＰＭが別のＴＰＭなら動作しない、非常に安全性の高い認証方法である。

【００２６】

第２の認証方法として、TPMとの組み合わせたパスワード認証があり、図４を使って説明する。

ステップ４１０において、Ｓｈａｄｏｗ　ＭＢＲ１０９はパスワードを含んだ暗号化データをＴＰＭ１０２に送る。具体的には、ＴＰＭの標準のＴＰＭ＿Ｕｎｓｅａｌコマンドを利用する。以下のステップ４２０から４４０まではＴＣＧ標準のＴＰＭの動作の一部であり、本発明にかかわる部分だけを説明する。

ステップ４２０において、ＴＰＭ１０２は受け取った暗号化データをＴＰＭ１０２内のみでアクセス可能な鍵を利用して復号する。

ステップ４３０において、ＴＰＭ１０２は復号したデータ中のＰＣＲ情報に関わる部分を現在のＰＣＲの状態と比較する。合致しなければ、エラーを返して処理を終了する。

本発明においては、現在のＰＣＲはステップ３１０で説明したＳｈａｄｏｗ　ＭＢＲ１０９のハッシュ値を含んでおり、合致するはずである。

ステップ４４０において、ＰＣＲ情報が合致していれば、ＴＰＭ１０２は復号したパスワードをＳｈａｄｏｗ　ＭＢＲ１０９に送り返す。

ステップ４５０において、Ｓｈａｄｏｗ　ＭＢＲ１０９はＴＰＭ１０２から受け取ったパスワードをハードディスクに送信して認証を行う。

なお、ステップ４１０においてＳｈａｄｏｗ　ＭＢＲ１０９がＴＰＭ１０２に送った暗号化データはＴＰＭ＿Ｓｅａｌコマンドを使って作成したものである。すなわち、パスワードをＴＰＭ１０２にある鍵で暗号化するのであるが、ＴＰＭ＿Ｕｎｓｅａｌを使った復号条件として、ＰＣＲがＳｈａｄｏｗ　ＭＢＲのハッシュ値を保持していることを指定してＴＰＭ＿Ｓｅａｌを使って暗号化した結果である。このためステップ４３０において、ＴＰＭ１０２はＰＣＲの状態を検査している。

【００２７】

本方法は第一の方法に比べれば、格段に安全になった。というのも、復号できる条件は、対応するＴＰＭ１０２を搭載したＰＣに限定され、かつ特定のＰＣＲの状態、すなわちＭＢＲのハッシュ値が特定の場合にのみ復号されるからである。これにより、特定のＰＣと特定のハードディスクの組み合わせのみで起動することになり、ハードディスクを別のＰＣにつないでもハードディスクに対する認証に失敗するので、アクセスできない。

しかしながら、ＰＣやメモリ、ＴＰＭ、ハードディスク間をやり取りされるデータにアクセスできる装置を持つ攻撃者には、パスワードが盗まれてしまう可能性がある。次の第三の方法はこれを防ぐ方法であり、さらに安全性が向上している。

なお、本認証方法を利用する場合、Shadow MBRのハッシュ値の計算は単純に全体のハッシュ値を求めるのではなく、暗号化データの部分をマスクしてＢＩＯＳ１０４がハッシュ値を計算する。

【００２８】

なお、本方法と類似の認証は、ＴＰＭの代わりに認証トークンでも可能である。すなわちパスワードを認証トークンの鍵で暗号化しておき、これをＳｈａｄｏｗ　ＭＢＲ１０９のプログラムが保持、ハードディスク認証時に認証トークンを使って復号してパスワードを取り出してハードディスクに送るのである。しかし、この方法では別のＰＣにハードディスクを接続、Ｓｈａｄｏｗ　ＭＢＲ１０９上の暗号化データを取り出し、これを認証トークンに渡してしまえば、パスワードが盗まれてしまう危険性があるので推奨できない。

以上がステップ３２０における第２の認証方法である。

【００２９】
第３の認証方法として、ＴＰＭ１０２との組み合わせた公開鍵暗号を利用した認証があり、図５を使って説明する。
ステップ５１０において、Ｓｈａｄｏｗ　ＭＢＲ１０９は秘密鍵を含んだ暗号化データをＴＰＭ１０２に送る。具体的には、ＴＰＭ１０２の標準のＴＰＭ＿ＬｏａｄＫｅｙ２コマンドを利用する。以下のステップ５２０から５４０までと５８０はＴＣＧ標準のＴＰＭの動作の一部、ステップ５６０はＴＣＧ　Ｓｔｏｒａｇｅ準拠のハードディスクの動作の一部であり、本発明にかかわる部分だけを説明する。
ステップ５２０において、ＴＰＭ１０２は受け取った暗号化データをＴＰＭ内で利用可能な鍵を利用して復号する。
ステップ５３０において、ＴＰＭ１０２は復号してデータ中のＰＣＲ情報に関わる部分を現在のＰＣＲの状態と比較する。合致しなければ、エラーを返して処理を終了する。本発明においては、現在のＰＣＲはステップ３１０で説明したＳｈａｄｏｗ　ＭＢＲ１０９のハッシュ値を含んでおり合致するはずである。
ステップ５４０において、ＰＣＲ情報が合致していれば、ＴＰＭ１０２は復号した秘密鍵を以下の処理で利用できるようにＴＰＭ１０２内に設定し、この鍵のハンドルをＳｈａｄｏｗ　ＭＢＲ１０９に送り返す。
【００３０】
ステップ５５０において、Ｓｈａｄｏｗ　ＭＢＲ１０９はＴＰＭ１０２から秘密鍵のハンドルを受け取った後、認証を始めることをハードディスク１０５に通知する。具体的にはＳｔａｒｔＳｅｓｓｉｏｎメソッドを起動する。
ステップ５６０において、認証に必要な乱数を生成、Ｓｈａｄｏｗ　ＭＢＲ１０９に送り返す。
ステップ５７０において、Ｓｈａｄｏｗ　ＭＢＲ１０９は乱数を受け取り、これデータに対する署名を生成するようにＴＰＭ１０２に送信する。具体的にはＴＰＭ＿Ｓｉｇｎコマンドを利用する。この際にステップ５５０で受け取ったハンドルを利用する。
ステップ５８０において、ＴＰＭ１０２は署名を生成、Ｓｈａｄｏｗ　ＭＢＲ１０９に送り返す。
ステップ５９０において、Ｓｈａｄｏｗ　ＭＢＲ１０９はＴＰＭ１０２から受け取った署名を、ハードディスク１０５に送り認証を行う。
【００３１】
なお、ステップ５１０においてＳｈａｄｏｗ　ＭＢＲ１０９がＴＰＭ１０２に送った暗号化データはＴＰＭ＿ＣｒｅａｔｅＷｒａｐＫｅｙコマンドを使って作成したものである。すなわち、秘密鍵をＴＰＭ１０２にある鍵で暗号化するのであるが、ＴＰＭ＿ＬｏａｄＫｅｙ２を使った復号条件として、ＰＣＲがＳｈａｄｏｗ　ＭＢＲのハッシュ値を保持していることを指定してＴＰＭ＿ＬｏａｄＫｅｙ２を使って暗号化した結果である。
なお本認証方法を利用する場合、Ｓｈａｄｏｗ　ＭＢＲ１０９のハッシュ値の計算は単純に全体のハッシュ値を求めるのではなく、暗号化データの部分をマスクしてＢＩＯＳ１０４がハッシュ値を計算する。
【００３２】
次にステップ３３０にて行うウィルス検索の概要を述べる。
第１のウィルス検索方法として、既存のウィルス検索方法と同様にウィルスのパターンを保持しておき、ハードディスク１０５上に本パターンが現れないか検索するものである。パターンは膨大な量がありＳｈａｄｏｗ　ＭＢＲ１０９中には格納できないので、ネットワークを経由しパターンを提供するサーバにアクセスして、パターンをダウンロードし、メモリ１０４上に格納して検索するものである。
【００３３】
第２のウィルス検索方法として、ハードディスク１０５全体を検索するのではなく、システムなど重要な部分のみを検索する方法である。重要な部分の例として、仮想化技術を用いたシステムにおけるゲストマシンではなく、ホストマシンないしはハイパーバイザに

あたる部分のみをウィルス検索対象とする方法がある。他にＯＳのカーネル部分のみなどが考えられる。検索方法としては、第一の方法と同様に、ウィルスパターンが含まれていないか検索するのが一般的である。

【００３４】

第３のウィルス検索方法として、検索を行うのではなく、ウィルスが含まれていないと保証されたディスクイメージをネットワーク経由でサーバからダウンロード、ハードディスクにコピーする方法がある。このコピーもハードディスク全体をコピーするのではなく、ＯＳやハイパーバイザなどシステム部分だけをコピーする方法もある。

【００３５】

図６を用いて、ウィルス検索と同時に実行可能なＰＣ起動制限処理の詳細を説明する。

ウィルスによる攻撃は、ＰＣ利用者が気がつかないうちにウィルスに感染してしまう場合がほとんどであるが、起動制限はＰＣ利用者本人の不正ないしは不注意によるＰＣ起動を制限するものである。起動が制限される例として、本実施形態では社内ネットワーク外での起動と社外での起動許可数を超えた起動を制限する例を示す。なお、ここで起動許可回数がＳｈａｄｏｗ　ＭＢＲ１０９の特定領域に保持されているとする。この特定領域は第二の認証方法と同様にＢＩＯＳプログラムによるハッシュ値の計算外となる。

【００３６】

ステップ６１０において、ステップ３２０と同様にしてＳｈａｄｏｗ　ＭＢＲ１０９にあるプログラムがハードディスク１０５に対して認証処理を行い、Ｓｈａｄｏｗ　ＭＢＲ１０９の書き換え可能モードに移行する。

ステップ６２０において、Ｓｈａｄｏｗ　ＭＢＲ１０９内に記録されている起動許可回数が１以上ならステップ６３０に飛ぶ。起動許可回数が０なら、原則起動禁止状態にあり、それでも起動可能かサーバに問い合わせ、起動ＯＫならステップ６４０に、ＮＧならステップ６５０に飛ぶ。

ステップ６３０において、Ｓｈａｄｏｗ　ＭＢＲ１０９の起動許可回数を１つ減じ、ステップ６４０に飛ぶ。

【００３７】

ステップ６４０において、Ｓｈａｄｏｗ　ＭＢＲ書き換え可能モードから書き換え禁止モードに移行して、ＭＢＲ１０８のブートストラップコードをメモリ１０３にロードし、制御を渡して、通常のブート処理を行う。

ステップ６５０において、Ｓｈａｄｏｗ　ＭＢＲ書き換え可能モードから書き換え禁止モードに移行して、起動を停止する。この際、ディスプレイに起動許可がなく停止した旨をメッセージ表示する。

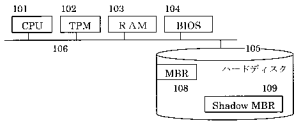
なお、本実施形態では、起動許可数がＳｈａｄｏｗ　ＭＢＲに記録されているが、Ｓｈａｄｏｗ　ＭＢＲは改ざんされる可能性があるため、それを防止するために、Ｓｈａｄｏｗ　ＭＢＲの起動回数は常に０としておいて、サーバに問い合わせるようにしても良い。また、Ｓｈａｄｏｗ　ＭＢＲではなく、認証後にアクセス可能なＭＢＲに記録するようにしても良い。さらに上記とは別の対策として、Ｓｈａｄｏｗ　ＭＢＲが改ざんされていないことを確認した後に、ＴＰＭ＿ＳｅａｌコマンドやＴＰＭ＿ＣｒｅａｔｅＷｒａｐｋｅｙコマンドでパスワードや鍵、PCR情報を含む暗号化データを暗号化しなおして、Ｓｈａｄｏｗ　ＭＢＲを書き直すようにしても良い。

【符号の説明】

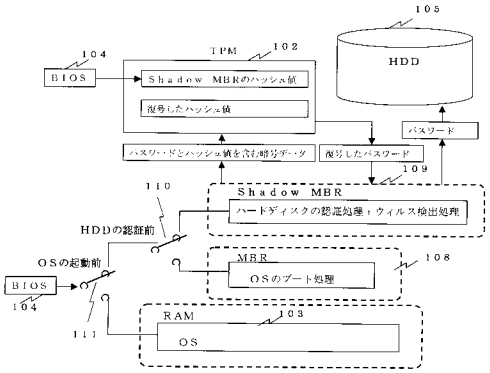
【００３８】

１０１：　ＣＰＵ
１０２：　ＴＰＭ
１０３：　メモリ
１０４：　ＢＩＯＳ
１０５：　ハードディスク
１０８：　ハードディスクへの認証後にアクセス可能なＭＢＲ
１０９：　ハードディスクへの認証前にアクセス可能なＳｈａｄｏｗ　ＭＢＲ

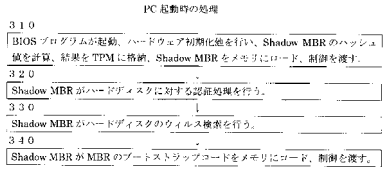
【図１】



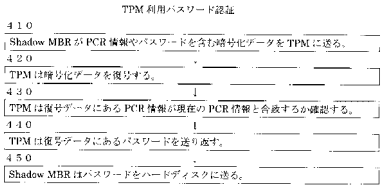
【図２】



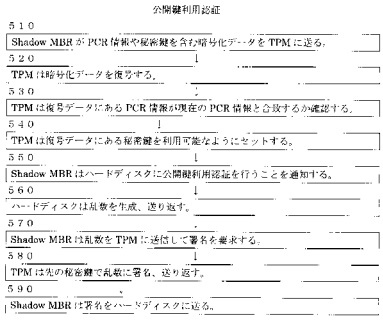
【図３】



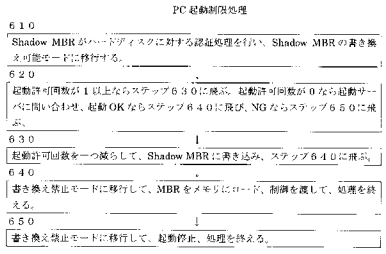
【図４】



【図５】



【図６】



フロントページの続き

(56)参考文献 特開２００６－０６５６８６（ＪＰ，Ａ）
特開２０００－１８１９６３（ＪＰ，Ａ）
特開２００９－１２９０６１（ＪＰ，Ａ）
国際公開第２００８／０８１８０１（WO，Ａ１）
特開２００８－１６５７５８（ＪＰ，Ａ）
特開２００６－２６８８６１（ＪＰ，Ａ）
特開２００４－０７８５３９（ＪＰ，Ａ）
特開２００７－２１９８０２（ＪＰ，Ａ）
特開平１０－３３３９０２（ＪＰ，Ａ）
特開２００４－０７２３３０（ＪＰ，Ａ）
特開２００６－２３６１９３（ＪＰ，Ａ）
特開２００８－２２６１９１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５６
Ｇ０６Ｆ　２１／１０