【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成20年11月20日(2008.11.20)

【公開番号】特開2006-178936(P2006-178936A)
【公開日】平成18年7月6日(2006.7.6)
【年通号数】公開・登録公報2006-026
【出願番号】特願2005-332691(P2005-332691)
【国際特許分類】
Ｇ０６Ｆ　21/22　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　9/06　　６６０Ｎ

【手続補正書】
【提出日】平成20年10月2日(2008.10.2)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピュータにおいて、前記コンピュータのエミュレートされた資源にそれぞれがアクセスする、自己完結型プロセス実行環境の複数のインスタンスをモニタし保護する方法であって、
有害なプロセスを検出するために自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれをモニタする少なくとも１つのセキュリティアプリケーションを、前記コンピュータ上で実行するステップであって、前記少なくとも１つのセキュリティアプリケーションは、自己完結型プロセス実行環境の前記複数のインスタンスの外部で実行されるステップと、
１組のセキュリティアプリケーションによって、自己完結型プロセス実行環境の前記複数のインスタンスの前記それぞれの仮想資源の走査を可能にするステップであって、自己完結型プロセス実行環境の前記複数のインスタンスの１つに関連付けられた仮想ネットワークアダプタ構造へのアクセス権を提供することを含むステップと、
を含み、
前記仮想資源は前記コンピュータのエミュレートされた資源を含み、
前記可能にするステップは、前記コンピュータの主オペレーティングシステムによって認識された前記資源を認識するように、前記１組のセキュリティアプリケーションを構成するステップを含むことを特徴とする方法。
【請求項２】
前記少なくとも１つのセキュリティアプリケーションは、自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれの中で１対１の対応関係で動作するそれに対応したエージェントセキュリティプロセスとの通信を介して、自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれにアクセスすることを特徴とする請求１に記載の方法。
【請求項３】
前記少なくとも１つのセキュリティアプリケーションは、前記少なくとも１つのセキュリティアプリケーションがそれを介して前記エミュレートされた資源にアクセスできる一様なインターフェースを提供する仮想マシンオブジェクトインターフェースを介して、自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれにアクセスすることを特徴とする請求項１に記載の方法。

【請求項４】
前記少なくとも１つのセキュリティアプリケーションは、前記コンピュータによって提供されるホストシステム中で実行され、自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれはまた、前記ホストシステム中で実行されることを特徴とする請求項１に記載の方法。
【請求項５】
前記少なくとも１つのセキュリティアプリケーションは、前記コンピュータによって提供されるホストシステム中で実行されること、自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれはまた、前記ホストシステム中で実行されること、ならびに前記少なくとも１つのセキュリティアプリケーションは、少なくとも一部分が、前記ホストシステム中で実行される監視プロセスによって制御されることを特徴とする請求項１に記載の方法。
【請求項６】
前記１組のセキュリティアプリケーションによって自己完結型プロセス実行環境の前記複数のインスタンスの前記それぞれの仮想資源の前記走査を可能にする前記ステップは、自己完結型プロセス実行環境の前記複数のインスタンスのうちの１つと関連付けられた仮想メモリ構造へのアクセス権を提供するステップを含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記１組のセキュリティアプリケーションによって自己完結型プロセス実行環境の前記複数のインスタンスの前記それぞれの仮想資源の走査を可能にする前記ステップは、自己完結型プロセス実行環境の前記複数のインスタンスのうちの１つと関連付けられた仮想ハードディスク構造へのアクセス権を提供するステップを含むことを特徴とする請求項１に記載の方法。
【請求項８】
コンピュータにおいて、前記コンピュータのエミュレートされた資源にそれぞれがアクセスする、自己完結型プロセス実行環境の複数のインスタンスをモニタし保護する方法であって、
有害なプロセスを検出するために自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれをモニタする少なくとも１つのセキュリティアプリケーションを、前記コンピュータ上で実行するステップであって、前記少なくとも１つのセキュリティアプリケーションは、自己完結型プロセス実行環境の前記複数のインスタンスの外部で実行されるステップと、
１組のセキュリティアプリケーションによって、自己完結型プロセス実行環境の前記複数のインスタンスの前記それぞれの仮想資源の走査を可能にするステップであって、自己完結型プロセス実行環境の前記複数のインスタンスのうちの１つと関連付けられた仮想ドライバ構造へのアクセス権を提供することを含むステップと、
を含み、
前記仮想資源は前記コンピュータのエミュレートされた資源を含み、
前記可能にするステップは、前記コンピュータの主オペレーティングシステムによって認識された前記資源を認識するように、前記１組のセキュリティアプリケーションを構成するステップを含むことを特徴とする方法。
【請求項９】
コンピュータにおいて、前記コンピュータのエミュレートされた資源にそれぞれがアクセスする、自己完結型プロセス実行環境の複数のインスタンスをモニタし保護する方法であって、
有害なプロセスを検出するために自己完結型プロセス実行環境の前記複数のインスタンスのそれぞれをモニタする少なくとも１つのセキュリティアプリケーションを、前記コンピュータ上で実行するステップであって、前記少なくとも１つのセキュリティアプリケーションは、自己完結型プロセス実行環境の前記複数のインスタンスの外部で実行されるス

テップと、
１組のセキュリティアプリケーションによって、自己完結型プロセス実行環境の前記複数のインスタンスの前記それぞれの仮想資源の走査を可能にするステップと、
を含み、
前記仮想資源は前記コンピュータのエミュレートされた資源を含み、
前記可能にするステップは、前記コンピュータの主オペレーティングシステムによって認識された前記資源を認識するように、前記１組のセキュリティアプリケーションを構成するステップを含み、
有害なプロセスが、自己完結型プロセス実行環境の前記複数のインスタンスのうちの１つで検出された場合、
まだ非活動化されていない場合、前記インスタンスを非活動化するステップと、
前記インスタンスを修復するステップと、
前記修復されたインスタンスを、活動化するために前記コンピュータのホスト環境にロードするステップと、
をさらに含むことを特徴とする方法。
【請求項１０】
望ましくないプロセスアクションによって生じた損害に対して、オペレーティングシステムを保護するためのコンピュータシステムにおける方法であって、
前記コンピュータシステムのインフラストラクチャのコアとなる諸態様（ｃｏｒｅ　ａｓｐｅｃｔｓ）から少なくとも部分的に隔離された前記オペレーティングシステム上で動作するカーネルを休止するステップと、
望ましくないプロセスアクションの兆候があるかどうかを判定するために前記カーネルを検査するステップであって、前記検査の少なくとも一部分は、前記少なくとも部分的に隔離されたオペレーティングシステムから独立している監視プロセスによって実施されるステップと、
前記少なくとも部分的に隔離されたオペレーティングシステム中に望ましくないプロセスアクションの兆候がある場合、前記望ましくないプロセスアクションを抑制する措置を講ずるステップと
を含むことを特徴とする方法。
【請求項１１】
前記望ましくないプロセスアクションを抑制する前記措置は、前記少なくとも部分的に隔離されたオペレーティングシステムを中断し、さらなるモニタリングを実施するステップを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記望ましくないプロセスアクションを抑制する前記措置は、前記少なくとも部分的に隔離されたオペレーティングシステム上で動作する選択プロセスを中断するステップことを含むことを特徴とする請求項１０に記載の方法。
【請求項１３】
前記望ましくないプロセスアクションを抑制する前記措置は、前記望ましくないプロセスアクションに関連するプロセスを終了させるステップを含むことを特徴とする請求項１０に記載の方法。
【請求項１４】
コンピュータシステムのコアコンポーネントに関連付けられた特権操作へのアクセス権を確保するためのコンピュータシステムであって、
プロセッサと、
前記プロセッサと通信する主メモリストレージと、
第２のストレージ装置と、
オペレーティングシステムと、
ホストシステムであって、
１つまたは複数の仮想マシンであり、前記１つまたは複数の仮想マシンのそれぞれが

、前記仮想マシンに関連付けられた環境中で動作するとき、有害なプロセスが直接前記コアコンポーネントにアクセスできないように前記コンピュータシステムの前記コアコンポーネントから隔離されていること、また前記１つまたは複数の仮想マシンのうちのそれぞれ１つが、仮想オペレーティングシステムのインスタンス、仮想メモリへのアクセス権、および少なくとも１つの仮想ドライバを含む仮想マシンと、

セキュリティアプリケーションと組み合わせて前記１つまたは複数の仮想マシンをモニタリングするのに使用される少なくとも１つの監視プロセスであり、前記モニタリングは有害プロセスの可能な検出を含み、また前記少なくとも１つの監視プロセスおよびセキュリティアプリケーションは前記仮想マシンから隔離されている監視プロセスと

を含むホストシステムと

を備えることを特徴とするシステム。

【請求項１５】

前記モニタリングはさらに、前記仮想メモリのアドレス空間のモニタリングを含むことを特徴とする請求項１４に記載のシステム。

【請求項１６】

前記仮想マシンはさらに、１つまたは複数のエミュレートされた装置へのアクセス権を含み、前記モニタリングはさらに、前記エミュレートされた装置のモニタリングを含むことを特徴とする請求項１４に記載のシステム。

【請求項１７】

前記仮想マシンはさらに、エミュレートされたハードドライブへのアクセス権を含み、前記モニタリングはさらに、前記エミュレートされたハードドライブのモニタリングを含むことを特徴とする請求項１４に記載のシステム。

【請求項１８】

前記モニタリングはさらに、前記仮想マシン上で動作するプロセスへの入力、またはプロセスからの出力に対して保全性の検証を実施することを含むことを特徴とする請求項１４に記載のシステム。

【請求項１９】

前記仮想マシンはさらに、エミュレートされたハードドライブへのアクセス権を含み、前記モニタリングはさらに、前記仮想メモリまたは前記エミュレートされたハードドライブ上に常駐するファイルの保全性を検査することを含むことを特徴とする請求項１４に記載のシステム。