【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27年1月29日(2015.1.29)

【公表番号】特表2013-545208(P2013-545208A)
【公表日】平成25年12月19日(2013.12.19)
【年通号数】公開・登録公報2013-068
【出願番号】特願2013-543292(P2013-543292)
【国際特許分類】
Ｇ０６Ｆ　9/46　(2006.01)
Ｇ０６Ｆ　21/56　(2013.01)
【ＦＩ】
Ｇ０６Ｆ　9/46　３５０
Ｇ０６Ｆ　21/00　１５６Ｅ

【手続補正書】
【提出日】平成26年12月3日(2014.12.3)
【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】
コンピューティング環境において、
バス・システムと、
前記バス・システムに接続された通信システムと、
前記バス・システムに接続されたメモリであって、該メモリはコンピュータ利用可能なプログラムコードを含む、メモリと、
前記バス・システムに接続された１又は複数の処理ユニットであって、該１又は複数の処理ユニットは前記コンピュータ利用可能なプログラムコードを実行して、仮想マシン環境において仮想マシンに対応する複数のゲスト・パーティションを作動させ、ゲスト・パーティションの各々がゲスト・アンチ・マルウェア・エージェントを含む、１又は複数の処理ユニットと、
１つまたは複数のアンチ・マルウェア関連のコンポーネントを含むアンチ・マルウェア・スキャン機構を実行するコンピュータ利用可能なプログラムコードであって、該アンチ・マルウェア・スキャン機構は前記ゲスト・パーティション上で前記ゲスト・アンチ・マルウェア・エージェントと通信するように構成され、さらに、共有アンチ・マルウェア・スキャン・リソースと共有アンチ・マルウェア・スキャン機能を、前記ゲスト・アンチ・マルウェア・エージェントを介して前記ゲスト・パーティションに提供するように構成され、前記ゲスト・アンチ・マルウェア・エージェントは前記スキャン機構に前記ゲスト・パーティション上の実行中のゲスト・オペレーティング・システム・リソースへのアクセスを提供するよう構成された、コンピュータ利用可能なプログラムコードと
を備えるシステム。
【請求項２】
ルート・パーティションに存在し、さらに前記仮想マシンを一時停止し、再開し、復旧し、再構築して感染のスキャンと是正を可能とするように構成され、前記ゲスト・エージェントを保護するように構成された管理コンポーネントを備える、請求項１に記載のシステム。
【請求項３】

前記アンチ・マルウェア・スキャン機構に接続された管理コンポーネントをさらに含み、該管理コンポーネントは前記アンチ・マルウェア・スキャン機構に仮想マシン管理サービスを提供するよう構成される、請求項１に記載のシステム。

【請求項４】

前記アンチ・マルウェア・スキャン機構が前記管理コンポーネントと通信して、前記管理サービスを使用してゲスト・パーティションを一時停止し、ゲスト・パーティションを再開し、ゲスト・パーティションのスナップショットを取得し、ゲスト・パーティションを過去の既知の良好なスナップショットにロールバックし、前記仮想マシンのイメージを再構築する、請求項３に記載のシステム。

【請求項５】

前記アンチ・マルウェア・スキャン機構が前記管理コンポーネントと通信して、前記アンチ・マルウェア・スキャニング機構によるスキャンのためにゲスト・パーティションをオフライン状態におく、請求項３に記載のシステム。

【請求項６】

前記アンチ・マルウェア・スキャン機構はさらに、署名の更新情報をリモートのデータ位置から取得するよう構成されている、請求項１に記載のシステム。

【請求項７】

前記アンチ・マルウェア・スキャン機構は、テレメトリ・データをリモートのデータ位置にアップロードし、または疑わしいコンテンツに関する決定を取得することに関してクラウド・サービスと通信するように構成され、または、テレメトリ・データをリモートのデータ位置にアップロードし、または疑わしいコンテンツに関する決定を取得することに関してクラウド・サービスと通信するようにさらに構成されていることの任意の組合せである、請求項１に記載のシステム。

【請求項８】

前記アンチ・マルウェア・スキャン機構は、前記アンチ・マルウェア・スキャン機構が前記共有アンチ・マルウェア・スキャン・リソース及び共有アンチ・マルウェア・スキャン機能を提供する前記ゲスト・パーティションとは別のゲスト・パーティションに存在する、請求項１に記載のシステム。

【請求項９】

前記アンチ・マルウェア・スキャン機構は前記仮想マシン環境のルート・パーティションに存在する、請求項１に記載のシステム。

【請求項１０】

前記共有アンチ・マルウェア・スキャン機能はゲスト・アンチ・マルウェア・エージェントと通信する１又は複数の命令を備え、前記ゲスト・アンチ・マルウェア・エージェントは前記１又は複数の命令を実行して前記スキャンと是正の実行を可能にするよう構成される、請求項１に記載のシステム。

【請求項１１】

コンピュータにより実行される方法であって、

少なくとも１つの処理ユニットにより、仮想マシン環境でメモリに格納された複数のゲスト・パーティションを仮想マシン環境で作動するステップであって、各ゲスト・パーティションはそのゲスト・パーティションで実行するゲスト・オペレーティング・システムとの相互作用を容易にするよう構成されたゲスト・アンチ・マルウェア・エージェントを作動する、ステップと、

前記少なくとも１つの処理ユニット上でアンチ・マルウェア・スキャン機構を実行するステップであって、該アンチ・マルウェア・スキャン機構は１又は複数のアンチ・マルウェア関連コンポーネントを備え、前記アンチ・マルウェア・スキャン機構は前記ゲスト・パーティション上で前記ゲスト・アンチ・マルウェア・エージェントと通信し、前記アンチ・マルウェア・スキャン機構は前記ゲスト・アンチ・マルウェア・エージェントを介して前記ゲスト・パーティションへ共有アンチ・マルウェア・スキャン機能を提供する、ステップと、

前記少なくとも１つの処理ユニット上で前記複数のゲスト・パーティションのうち１つのゲスト・パーティションをスキャンまたは復元するために、共有オーケストレーション機構を実行するステップと
を含む方法。
【請求項１２】
前記共有オーケストレーション機構を実行するステップが、
ゲスト・パーティションをオフライン状態にし、前記オフライン状態中に前記オフラインのゲスト・パーティションをスキャンし、前記オフライン状態に対して任意の必要な是正措置を取るステップを含む、請求項１１に記載の方法。
【請求項１３】
前記共有オーケストレーション機構を実行するステップが、
前記共有オーケストレーション機構とスキャン・コンポーネントとの間で通信してゲスト・パーティションを過去の状態に復元するステップを含む、請求項１１に記載の方法。
【請求項１４】
ゲスト・アンチ・マルウェア・エージェントをゲスト・パーティション上で作動させるステップと、前記ゲスト・エージェントにより提供されたデータをスキャン機構で受け取るステップと、前記データを前記スキャン機構でスキャンするステップと、スキャン結果に対応する情報を前記ゲスト・エージェントに返すステップとをさらに含む、請求項１１に記載の方法。
【請求項１５】
前記データを受け取るステップと前記データをスキャンするステップとが、リアルタイムな監視動作を実施するステップを含む、請求項１４に記載の方法。
【請求項１６】
スキャンすべき少なくとも１つのオブジェクトを要求する命令を含めて、前記ゲスト・アンチ・マルウェア・エージェントが実行するための命令を前記スキャン機構から前記ゲスト・アンチ・マルウェア・エージェントに提供するステップをさらに含む、請求項１４に記載の方法。
【請求項１７】
前記ゲスト・アンチ・マルウェア・エージェントが実施するための是正措置を指定する少なくとも１つの命令を含めて、前記ゲスト・アンチ・マルウェア・エージェントが実行するための命令を前記スキャン機構から前記ゲスト・アンチ・マルウェア・エージェントに提供するステップをさらに含む、請求項１４に記載の方法。
【請求項１８】
コンピュータ利用可能なプログラムコード格納したシステム・メモリであって、該プログラムコードは
仮想マシン環境において複数のゲスト・パーティションを実行するための命令であって、ゲスト・パーティションの各々がゲスト・アンチ・マルウェア・エージェントを含む、命令と、
１つまたは複数のアンチ・マルウェア関連のコンポーネントを含むアンチ・マルウェア・スキャン機構を実行する命令であって、該アンチ・マルウェア・スキャン機構は前記ゲスト・パーティション上で前記ゲスト・アンチ・マルウェア・エージェントと通信するように構成され、さらに、共有アンチ・マルウェア・スキャン・リソースと共有アンチ・マルウェア・スキャン機能を、前記ゲスト・アンチ・マルウェア・エージェントを介して前記ゲスト・パーティションに提供するように構成されている、命令と、
前記ゲスト・アンチ・マルウェア・エージェントを保護するための管理コンポーネントを構成するための命令であって、該管理コンポーネントはルート・パーティションに存在し、さらに前記仮想マシンを一時停止し、再開し、復旧し、再構築してスキャンと感染の是正を可能にするように構成されている、命令と、
を備えるシステム・メモリ。