(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2010-73011
(P2010-73011A)
(43)公開日　平成22年4月2日(2010.4.2)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660N	5B276
G06F 9/46	(2006.01)	G06F	9/46	350	

審査請求 未請求　請求項の数 10　ＯＬ　（全 13 頁）

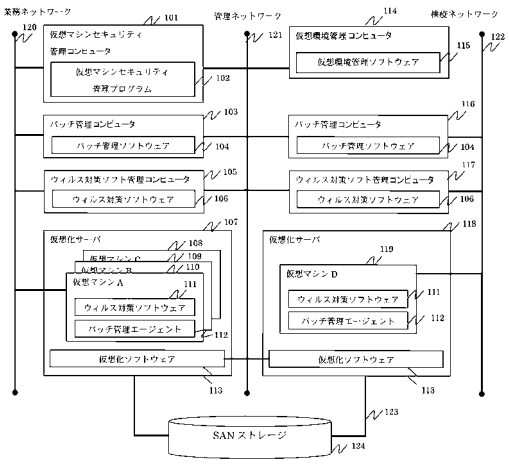
(21)出願番号　特願2008-240985 (P2008-240985)
(22)出願日　平成20年9月19日 (2008.9.19)

(71)出願人　000152985
株式会社日立情報システムズ
東京都品川区大崎１－２－１
(74)代理人　100074550
弁理士　林　實
(74)代理人　110000073
特許業務法人プロテック
(72)発明者　渡邊　淳弘
東京都品川区大崎１－２－１　株式会社日立情報システムズ内
(72)発明者　大島　義明
東京都品川区大崎１－２－１　株式会社日立情報システムズ内

Ｆターム(参考)　5B276 FD08　FD09

(54)【発明の名称】仮想マシンセキュリティ管理システム及び仮想マシンセキュリティ管理方法

(57)【要約】
【課題】仮想化環境におけるセキュリティの向上。
【解決手段】仮想マシンセキュリティ管理コンピュータ１０１が、ユーザ要求又はウィルス感染検知又はセキュリティパッチ未適用によるメッセージが発せられたとき、検疫用に準備した検疫用仮想化サーバ１１８に検疫用仮想マシン１１９を生成し、この生成した検疫用仮想マシン１１９の元となるテンプレートが検疫済みか否かを判定し、検疫に合格した仮想マシン１１９を検疫用仮想化サーバ１０７から実稼動環境の稼動仮想化サーバ１０７に移動することによって、ウィルス感染がなく且つセキュリティパッチの当てられた仮想マシンを生成する。
【選択図】図１



【特許請求の範囲】
【請求項１】
プログラムを実行する複数の仮想マシンを稼動させる複数の稼動仮想化サーバと、
前記プログラムのウィルス感染を検知するウィルス対策ソフトウェア及び前記プログラムの保安上の弱点を修正する修正プログラムが最新か否かを判定するパッチ管理ソフトウェアとを実行する検疫用仮想マシンを稼動させる検疫用仮想化サーバと、
前記複数の仮想マシンのプログラム構成情報をテンプレートとして格納し、仮想マシンを制御する仮想環境管理コンピュータと、
前記仮想マシンのウィルス感染に関するセキュリティを管理する仮想マシンセキュリティ管理コンピュータとを備えたコンピュータシステムの仮想マシンセキュリティ管理システムであって、
前記仮想マシンセキュリティ管理コンピュータが、
複数のメッセージに対応した対策処理の識別子を格納するメッセージマスタテーブルと、前記稼動仮想化サーバ上で稼動させる稼動仮想マシンのテンプレートの識別子及び該テンプレートが検疫済みか否かの検疫フラグを格納する仮想マシンマスタテーブルと、複数の稼動仮想化サーバ上で稼動させている稼動仮想マシンの搭載数を格納するホストマシンマスタテーブルと、前記メッセージマスタテーブルと仮想マシンマスタテーブルとホストマシンマスタテーブルの情報を参照して検疫用仮想化サーバ上に検疫用仮想マシンを生成する制御部とを有し、
該制御部が、新たに仮想マシンを生成するメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき、
前記仮想環境管理コンピュータのテンプレートを参照して前記検疫用仮想化サーバ上に、検疫用仮想マシンを生成する第１工程と、
該第１工程により生成した検疫用仮想マシンのテンプレートが検疫済みか否かを前記仮想マシンマスタテーブルの検疫フラグを参照して判定する第２工程と、
該第２工程において生成した検疫用仮想マシンのテンプレートが検疫済みと判定したとき、検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動する第３工程とを実行する仮想マシンセキュリティ管理システム。
【請求項２】
前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのウィルス対策ソフトウェアからウィルス感染のメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき、
前記第１工程から第２工程に移行する間に、前記第１工程により生成した検疫用仮想マシンのウィルス対策ソフトウェア及びパッチ管理ソフトウェアにより、ウィルス感染の有無及びセキュリティパッチが最新か否かを判定し、ウィルス感染がなく且つ最新のセキュリティパッチと判定したときに前記第２工程に移行する第４工程を実行する請求項１記載の仮想マシンセキュリティ管理システム。
【請求項３】
前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのパッチ管理ソフトウェアからパッチ未適用とのメッセージであることを前記メッセージマスタテーブルの識別子を参照して判定したとき、
前記第１工程から第２工程に移行する間に、前記メッセージを発した稼動仮想マシンを前記稼動仮想化サーバ上から削除する第５工程を実行する請求項１記載の仮想マシンセキュリティ管理システム。
【請求項４】
前記仮想マシンセキュリティ管理コンピュータの制御部が、新たな仮想マシンの生成又はウィルス感染又はパッチ未適用のメッセージ以外のメッセージを受けたとき、
前記第１工程から第３工程を実行する請求項１記載の仮想マシンセキュリティ管理システム。
【請求項５】

前記仮想マシンセキュリティ管理コンピュータの制御部が、前記第３工程により前記検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動するとき、前記ホストマシンマスタテーブルを参照し、稼動している稼動仮想マシン搭載数の数が最も少ない稼動仮想化サーバに、前記検疫用仮想マシンを移動させる請求項１から４何れかに記載の仮想マシンセキュリティ管理システム。

【請求項６】

プログラムを実行する複数の仮想マシンを稼動させる複数の稼動仮想化サーバと、

前記プログラムのウィルス感染を検知するウィルス対策ソフトウェア及び前記プログラムの保安上の弱点を修正する修正プログラムが最新か否かを判定するパッチ管理ソフトウェアとを実行する検疫用仮想マシンを稼動させる検疫用仮想化サーバと、

前記複数の仮想マシンのプログラム構成情報をテンプレートとして格納し、仮想マシンを制御する仮想環境管理コンピュータと、

前記仮想マシンのウィルス感染に関するセキュリティを管理する仮想マシンセキュリティ管理コンピュータとを備えたコンピュータシステムの仮想マシンセキュリティ管理方法であって、

前記仮想マシンセキュリティ管理コンピュータに、

複数のメッセージに対応した対策処理の識別子を格納するメッセージマスタテーブルと、前記稼動仮想化サーバ上で稼動させる稼動仮想マシンのテンプレートの識別子及び該テンプレートが検疫済みか否かの検疫フラグを格納する仮想マシンマスタテーブルと、複数の稼動仮想化サーバ上で稼動させている稼動仮想マシンの搭載数を格納するホストマシンマスタテーブルと、前記メッセージマスタテーブルと仮想マシンマスタテーブルとホストマシンマスタテーブルの情報を参照して検疫用仮想化サーバ上に検疫用仮想マシンを生成する制御部とを設け、

該制御部が、新たに仮想マシンを生成するメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき、

前記仮想環境管理コンピュータのテンプレートを参照して前記検疫用仮想化サーバ上に、検疫用仮想マシンを生成する第１工程と、

該第１工程により生成した検疫用仮想マシンのテンプレートが検疫済みか否かを前記仮想マシンマスタテーブルの検疫フラグを参照して判定する第２工程と、

該第２工程において生成した検疫用仮想マシンのテンプレートが検疫済みと判定したとき、検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動する第３工程とを実行する仮想マシンセキュリティ管理方法。

【請求項７】

前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのウィルス対策ソフトウェアからウィルス感染のメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき

前記第１工程から第２工程に移行する間に、前記第１工程により生成した検疫用仮想マシンのウィルス対策ソフトウェア及びパッチ管理ソフトウェアにより、ウィルス感染の有無及びセキュリティパッチが最新か否かを判定し、ウィルス感染がなく且つ最新のセキュリティパッチと判定したときに前記第２工程に移行する第４工程を実行する請求項５記載の仮想マシンセキュリティ管理方法。

【請求項８】

前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのパッチ管理ソフトウェアからパッチ未適用とのメッセージであることを前記メッセージマスタテーブルの識別子を参照して判定したとき、

前記第１工程から第２工程に移行する間に、前記メッセージを発した稼動仮想マシンを前記稼動仮想化サーバ上から削除する第５工程を実行する請求項６記載の仮想マシンセキュリティ管理方法。

【請求項９】

前記仮想マシンセキュリティ管理コンピュータの制御部が、新たな仮想マシンの生成又

はウィルス感染又はパッチ未適用のメッセージ以外のメッセージを受けたとき、
前記第１工程から第３工程を実行する請求項６記載の仮想マシンセキュリティ管理方法。
【請求項１０】
前記仮想マシンセキュリティ管理コンピュータの制御部が、前記第３工程により前記検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動するとき、前記ホストマシンマスタテーブルを参照し、稼動している稼動仮想マシン搭載数の数が最も少ない稼動仮想化サーバに、前記検疫用仮想マシンを移動させる請求項６から９何れかに記載の仮想マシンセキュリティ管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、仮想化ソフトウェアによりエミュレートされた仮想マシンと呼ばれる擬似的なマシン環境を使用したコンピュータシステムにおける仮想マシンセキュリティ管理システム及び仮想マシンセキュリティ管理方法に係り、特にウィルス対策ソフトやパッチ管理ソフトなどのセキュリティ検疫ソフトの検疫結果を踏まえた環境下で仮想マシンを運用することができる仮想マシンセキュリティ管理システム及び仮想マシンセキュリティ管理方法に関する。
【背景技術】
【０００２】
近年の企業等においては、運用コストの削減などを目的として仮想化ソフトウェアなどを使用し、１台のハードウェア上で複数のオペレーティングシステムを稼動させる仮想マシンを提供している。また、情報漏えい防止などを目的として、データセンタ内にクライアント端末として仮想マシンを用意し、ハードディスクやＣＤドライブなど媒体に情報を記録する仕組みを持たないシンクライアント端末からアクセスするソリューションも注目を集めている。ここでの仮想化ソフトウェアとは、オペレーティングシステムが制御するハードウェアを擬似的に作り出すソフトウェアをいう。一般的な仮想化ソフトウェアとしては、ＶＭｗａｒｅ（登録商標）ＥＳＸ　Ｓｅｒｖｅｒ（ＶＭｗａｒｅ社によって提供されるソフトウェア）、Ｍｉｃｒｏｓｏｆｔ（登録商標）　Ｈｙｐｅｒ－Ｖ（登録商標）（Ｍｉｃｒｏｓｏｆｔ社によって提供されるソフトウェア）などが相当する。
【０００３】
一般に仮想マシンのセキュリティに関する運用は、１台のハードウェア上に１つのオペレーティングシステムを配置する一般的なマシン環境と同様に、その仮想マシン上にウィルス対策ソフトを常駐させて定期的に自マシンのセキュリティチェックを行う方法や、ソフトウェアに保安上の弱点(セキュリティホール)が発覚した時に配布される修正プログラムであるセキュリティパッチのパッチ管理用マシンと監視対象マシンに常駐させたエージェント（ソフトウェア）とを用意し、パッチ管理用マシンが監視対象マシンのセキュリティパッチが当たっているか否か（最新の修正プログラムが当てられているか否か）を検査する方法が採用されている。
【０００４】
尚、仮想マシンのセキュリティに関する技術が記載された文献にとして例えば下記特許文献１が挙げられ、この特許文献１には、仮想マシンと仮想スイッチからなる仮想ネットワークシステムを構成させ、サーバの仮想マシンソフトウェアによる検査に合格しなければ検査対象のコンピュータを起動できないようにすることによって、検査対象のコンピュータの外部から検査を実施する検疫ネットワークシステム技術が記載されている。
【特許文献１】特開２００８－９０７９１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
前述の従来技術による仮想マシンのセキュリティ技術は、仮想マシン稼働中にウィルス

対策ソフトの検疫によりウィルス感染が確認された場合、オペレーティングシステムを再インストールすることや、感染前の状態にリカバリすることや、あるいはウィルス対策ソフトを開発する会社が公開する手順に従って手動で駆除することなどが必要である。しかし、これら対策は管理者又はユーザが手動で操作しなければならないため、対応の遅れや対策漏れなどによりウィルスの感染を拡大させる危険があると言う不具合があった。

【０００６】

また従来技術によるパッチ管理ソフトウェアによるセキュリティパッチの確認を行う技術は、セキュリティパッチの未適用が検出された場合、管理者又はユーザの手作業によりパッチを適用させる作業や、パッチ管理ソフトウェアにより指定パッチを強制的に適用する作業が必要になる。前者の場合、対応の遅れやパッチの適用漏れが発生し、クラッカーやウィルスの攻撃を容易にする可能性があり、後者の場合、ユーザがマシンを使用しているときに強制的に再起動され、マシンが提供するサービスが利用できないといった不具合があった。

【０００７】

本発明の目的は、仮想化ソフトウェアが有する仮想マシンの複製機能、仮想マシンのハードウェア間移動機能を利用し、ウィルス対策ソフトやパッチ管理ソフトウェアの検疫結果を元に、ユーザが定義するセキュリティ条件を満たした環境下で仮想マシンを稼働させることができる仮想マシンセキュリティ管理システム及び仮想マシンセキュリティ管理方法を提供することである。

【課題を解決するための手段】

【０００８】

前記目的を達成するために本発明は、

プログラムを実行する複数の仮想マシンを稼動させる複数の稼動仮想化サーバと、

前記プログラムのウィルス感染を検知するウィルス対策ソフトウェア及び前記プログラムの保安上の弱点を修正する修正プログラムが最新か否かを判定するパッチ管理ソフトウェアとを実行する検疫用仮想マシンを稼動させる検疫用仮想化サーバと、

前記複数の仮想マシンのプログラム構成情報をテンプレートとして格納し、仮想マシンを制御する仮想環境管理コンピュータと、

前記仮想マシンのウィルス感染に関するセキュリティを管理する仮想マシンセキュリティ管理コンピュータとを備えたコンピュータシステムの仮想マシンセキュリティ管理システムであって、

前記仮想マシンセキュリティ管理コンピュータが、

複数のメッセージに対応した対策処理の識別子を格納するメッセージマスタテーブルと、前記稼動仮想化サーバ上で稼動させる稼動仮想マシンのテンプレートの識別子及び該テンプレートが検疫済みか否かの検疫フラグを格納する仮想マシンマスタテーブルと、複数の稼動仮想化サーバ上で稼動させている稼動仮想マシンの搭載数を格納するホストマシンマスタテーブルと、前記メッセージマスタテーブルと仮想マシンマスタテーブルとホストマシンマスタテーブルの情報を参照して検疫用仮想化サーバ上に検疫用仮想マシンを生成する制御部とを有し、

該制御部が、新たに仮想マシンを生成するメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき、

前記仮想環境管理コンピュータのテンプレートを参照して前記検疫用仮想化サーバ上に、検疫用仮想マシンを生成する第１工程と、

該第１工程により生成した検疫用仮想マシンのテンプレートが検疫済みか否かを前記仮想マシンマスタテーブルの検疫フラグを参照して判定する第２工程と、

該第２工程において生成した検疫用仮想マシンのテンプレートが検疫済みと判定したとき、検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動する第３工程とを実行することを第１の特徴とする。

【０００９】

また本発明は、第１の特徴の仮想マシンセキュリティ管理システムにおいて、前記仮想

マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのウィルス対策ソフトウェアからウィルス感染のメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき

前記第１工程から第２工程に移行する間に、前記第１工程により生成した検疫用仮想マシンのウィルス対策ソフトウェア及びパッチ管理ソフトウェアにより、ウィルス感染の有無及びセキュリティパッチが最新か否かを判定し、ウィルス感染がなく且つ最新のセキュリティパッチと判定したときに前記第２工程に移行する第４工程を実行することを第２の特徴とする。

【００１０】

また本発明は、第１の特徴の仮想マシンセキュリティ管理システムにおいて、前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのパッチ管理ソフトウェアからパッチ未適用とのメッセージであることを前記メッセージマスタテーブルの識別子を参照して判定したとき、

前記第１工程から第２工程に移行する間に、前記メッセージを発した稼動仮想マシンを前記稼動仮想化サーバ上から削除する第５工程を実行することを第３の特徴とする。

【００１１】

また本発明は、第１の特徴の仮想マシンセキュリティ管理システムにおいて、前記仮想マシンセキュリティ管理コンピュータの制御部が、新たな仮想マシンの生成又はウィルス感染又はパッチ未適用のメッセージ以外のメッセージを受けたとき、前記第１工程から第３工程を実行することを第４の特徴とする。

【００１２】

また本発明は、前記何れかの特徴の仮想マシンセキュリティ管理システムにおいて、前記仮想マシンセキュリティ管理コンピュータの制御部が、前記第３工程により前記検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動するとき、前記ホストマシンマスタテーブルを参照し、稼動している稼動仮想マシン搭載数の数が最も少ない稼動仮想化サーバに、前記検疫用仮想マシンを移動させることを第５の特徴とする。

【００１３】

更に本発明は、

プログラムを実行する複数の仮想マシンを稼動させる複数の稼動仮想化サーバと、

前記プログラムのウィルス感染を検知するウィルス対策ソフトウェア及び前記プログラムの保安上の弱点を修正する修正プログラムが最新か否かを判定するパッチ管理ソフトウェアとを実行する検疫用仮想マシンを稼動させる検疫用仮想化サーバと、

前記複数の仮想マシンのプログラム構成情報をテンプレートとして格納し、仮想マシンを制御する仮想環境管理コンピュータと、

前記仮想マシンのウィルス感染に関するセキュリティを管理する仮想マシンセキュリティ管理コンピュータとを備えたコンピュータシステムの仮想マシンセキュリティ管理方法であって、

前記仮想マシンセキュリティ管理コンピュータに、

複数のメッセージに対応した対策処理の識別子を格納するメッセージマスタテーブルと、前記稼動仮想化サーバ上で稼動させる稼動仮想マシンのテンプレートの識別子及び該テンプレートが検疫済みか否かの検疫フラグを格納する仮想マシンマスタテーブルと、複数の稼動仮想化サーバ上で稼動させている稼動仮想マシンの搭載数を格納するホストマシンマスタテーブルと、前記メッセージマスタテーブルと仮想マシンマスタテーブルとホストマシンマスタテーブルの情報を参照して検疫用仮想化サーバ上に検疫用仮想マシンを生成する制御部とを設け、

該制御部が、新たに仮想マシンを生成するメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき、

前記仮想環境管理コンピュータのテンプレートを参照して前記検疫用仮想化サーバ上に、検疫用仮想マシンを生成する第１工程と、

該第１工程により生成した検疫用仮想マシンのテンプレートが検疫済みか否かを前記仮想マシンマスタテーブルの検疫フラグを参照して判定する第２工程と、
該第２工程において生成した検疫用仮想マシンのテンプレートが検疫済みと判定したとき、検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動する第３工程とを実行することを第６の特徴とする。

【００１４】

また本発明は、第６の特徴の仮想マシンセキュリティ管理方法において、前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのウィルス対策ソフトウェアからウィルス感染のメッセージを受けたことを前記メッセージマスタテーブルの識別子を参照して判定したとき前記第１工程から第２工程に移行する間に、前記第１工程により生成した検疫用仮想マシンのウィルス対策ソフトウェア及びパッチ管理ソフトウェアにより、ウィルス感染の有無及びセキュリティパッチが最新か否かを判定し、ウィルス感染がなく且つ最新のセキュリティパッチと判定したときに前記第２工程に移行する第４工程を実行することを第６の特徴とする。

【００１５】

また本発明は、第６の特徴の仮想マシンセキュリティ管理方法において、前記仮想マシンセキュリティ管理コンピュータの制御部が、稼動仮想マシンのパッチ管理ソフトウェアからパッチ未適用とのメッセージであることを前記メッセージマスタテーブルの識別子を参照して判定したとき、前記第１工程から第２工程に移行する間に、前記メッセージを発した稼動仮想マシンを前記稼動仮想化サーバ上から削除する第５工程を実行することを第８の特徴とする。

【００１６】

また本発明は、第６の特徴の仮想マシンセキュリティ管理方法において、前記仮想マシンセキュリティ管理コンピュータの制御部が、新たな仮想マシンの生成又はウィルス感染又はパッチ未適用のメッセージ以外のメッセージを受けたとき、前記第１工程から第３工程を実行することを第９の特徴とする。

【００１７】

また本発明は、前記何れかの特徴の仮想マシンセキュリティ管理方法において、前記仮想マシンセキュリティ管理コンピュータの制御部が、前記第３工程により前記検疫用仮想化サーバ上の検疫用仮想マシンを稼動仮想化サーバ上に稼動仮想マシンとして移動するとき、前記ホストマシンマスタテーブルを参照し、稼動している稼動仮想マシン搭載数の数が最も少ない稼動仮想化サーバに、前記検疫用仮想マシンを移動させることを第１０の特徴とする。

【発明の効果】

【００１８】

本発明による仮想マシンセキュリティ管理システム及び仮想マシンセキュリティ管理方法は、ユーザ要求又はウィルス感染検知又はセキュリティパッチ未適用によるメッセージが発せられたとき、検疫用に準備した検疫用仮想化サーバに検疫用仮想マシンを生成し、この生成した検疫用仮想マシンの元となるテンプレートが検疫済みか否かを判定し、検疫に合格した仮想マシンを検疫用仮想化サーバから実稼動環境の稼動仮想化サーバに移動することによって、ウィルス感染がなく且つセキュリティパッチの当てられた仮想マシンを生成することができる。

【発明を実施するための最良の形態】

【００１９】

以下、本発明による仮想マシンセキュリティ管理方法を適用した仮想マシンセキュリティ管理システムを図面を参照して説明する。図１は、本発明の一実施形態による仮想マシンセキュリティ管理システムを適用したコンピュータシステムの全体構成図、図２は、本実施形態による仮想マシンセキュリティ管理システムの構成を示す図、図３は、本実施形態による各種データテーブルの構成を説明するための図、図４は、本実施形態によるメッセージ解析部の動作フローチャート図、図５は、本実施形態による仮想マシン作成処理部

の動作フローチャート図である。

【００２０】

［構成］

［全体構成］

本実施形態による仮想マシンセキュリティ管理システムが適用されるコンピュータシステムの全体構成は、図１に示す如く、複数の仮想マシン１０８～１１０を仮想化ソフトウェア１１３により稼動させる（稼動）仮想化サーバ１０７と、該仮想化サーバ１０７の仮想マシン１１０のウィルス対策ソフトウェア１１１を管理するためのウィルス対策ソフトウェア１０６を搭載するウィルス対策ソフトウェア管理コンピュータ１０５と、前記仮想化サーバ１０７の仮想マシン１１０のパッチ管理エージェント（ソフトウェア）１１２を管理するためのパッチ管理ソフトウェア１０４を搭載するパッチ管理コンピュータ１０３と、本実施形態によるセキュリティ管理用の仮想マシン１１９を仮想化ソフトウェア１１３により動作させる仮想化サーバ１１８と、該仮想マシン１１９のウィルス対策ソフトウェア１１１を管理するためのウィルス対策ソフトウェア１０６を搭載するウィルス対策ソフトウェア管理コンピュータ１１７と、前記仮想化サーバ１１８の仮想マシン１１９のパッチ管理エージェント１１２を管理するためのパッチ管理ソフトウェア１０４を搭載するパッチ管理コンピュータ１１６と、本実施形態の特徴である仮想マシンセキュリティ管理プログラム１０２を搭載した仮想マシンセキュリティ管理コンピュータ１０１と、前述の仮想化サーバ１０７及び１１８による仮想マシンの仮想化環境を制御するための仮想環境管理ソフトウェア１１５を搭載する仮想環境管理コンピュータ１１４と、前記仮想化サーバ１０７及び１１８に接続され、仮想マシンのデータ記憶を行うためのＳＡＮ（Ｓｔｏｒａｇｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）ストレージ１２４と、前記コンピュータやサーバを接続する業務ネットワーク１２０／管理ネットワーク１２１／検疫ネットワーク１２２とから構成され、これらネットワークは個々に分離されている。前記仮想マシンセキュリティ管理プログラム１０２を搭載した仮想マシンセキュリティ管理コンピュータ１０１は、パッチ管理ソフトウェア１０４により、監視対象の仮想マシンに埋め込まれたパッチ管理エージェント１１２を使用してパッチ適用状況を監視するものであり、前記仮想環境管理コンピュータ１１４は、仮想環境と仮想マシンを管理し、仮想マシンをリソース使用状況の低いホストマシン上に自動で立ち上げるＡＰＩを搭載したソフトウェアが稼動するサーバをいう。一般的な仮想環境管理ソフトウェアとしては、ＶＭｗａｒｅ（登録商標） ＶｉｒｔｕａｌＣｅｎｔｅｒ（ＶＭｗａｒｅ社によって提供されるソフトウェア）、ＶＭｗａｒｅ（登録商標） Ｖｉｒｔｕａｌ Ｄｅｓｋｔｏｐ Ｍａｎａｇｅｒ ２（ＶＭｗａｒｅ社によって提供されるソフトウェア）などが好適であるが、これに限られるものではない。また図１においては、仮想化サーバ１０７が１台の例を図示しているが、本実施形態においては複数の仮想化サーバが接続されているものとする。

【００２１】

［仮想マシンセキュリティ管理コンピュータ１０１］

本実施形態の特徴である仮想マシンセキュリティ管理コンピュータ１０１の機能的構成は、図２示す如く、ユーザからの処理要求あるいはウィルス対策ソフトやパッチ管理エージェント１１２からの警告を受け付けるデータ通信部２０２と、処理要求または警告に対して必要な処理を判断するメッセージ解析部２０３と、仮想マシンを作成し検疫を実行後、実運用環境へ仮想マシンを移動させる仮想マシン作成処理部２０４と、ウィルス感染時などに仮想マシンを削除する仮想マシン削除処理部２０５と、定期的に仮想マシンの配置状況を監視する仮想マシン情報同期処理部２０６と、処理要求または警告の種類を判別するためのメッセージマスタテーブル２０７と、仮想マシンを構成するテンプレートであるかとどうか、または検疫済みであるかどうかの情報を格納する仮想マシンマスタテーブル２０８と、仮想マシンを稼動させるホストマシンマスタテーブル２０９とを備える。

【００２２】

［データテーブル］

前記メッセージマスタテーブル２０７に格納される情報は、図３（Ａ）に示す如く、識

別子であるＩＤ３０１と、メッセージ名称３０２と、該メッセージに対応した対処方法に対応して付与された対応処理ＩＤ３０３の各項目情報とから構成され、例えば、ＩＤ「０００１」のメッセージ名称「ウィルス感染警告」に対して対策処理ＩＤが「１」の如く登録されているものであって、ウィルス対策ソフトやパッチ管理エージェント１１２からの警告、あるいは仮想マシンを新規作成する際に出されるユーザの要求など複数あるメッセージを、ウィルス対策ソフトからの警告、パッチ管理エージェントからの警告、及びユーザからの要求の３つに分類するためのテーブルである。

【００２３】

前記仮想マシンマスタテーブル２０８に格納される情報は、図３（ｂ）に示す如く、識別子であるＩＤ３０４と、仮想マシン名称３０５と、該仮想マシンのＩＰアドレス３０６と、該仮想マシンを稼働するホストのＩＤ３０７と、その仮想マシンがテンプレートであるかどうかを示すテンプレートフラグ３０８と、どのテンプレートから作成された仮想マシンなのかを示す作成元テンプレート３０９と、既に検疫を受けているかどうかを示す検疫フラグ３１０との各項目情報とから構成され、例えばＩＤ「１」の名称が「ＡＢＣ」の仮想マシンが、ＩＰアドレスが「１９２．１６８．０．１」、ホストＩＤが「０００１」、テンプレートフラグが「１」（テンプレートであることを示す）、作成元テンプレートがなく、検疫フラグが「０」（検疫されていない）と登録され、ＩＤ「２」の名称が「ＤＥＦ」の仮想マシンが、ＩＰアドレスが「１９２．１６８．０．２」、ホストＩＤが「０００１」、テンプレートフラグが「０」（テンプレートでないことを示す）、作成元テンプレートが「ＡＢＣ」、検疫フラグが「１」（検疫済みである）と登録されている。これにより、ウィルス感染時などに仮想マシンの代替マシンとして、現状と同じ機能を有するものを用意することができる。また、検疫フラグがあることで、ウィルス感染の恐れがないテンプレートに関して何度も検疫を行うことを防止することができる。

【００２４】

前記ホストマシンマスタテーブル２０９は、識別子であるＩＤ３１１と、仮想マシン稼動させるホストの名称３１２と、該ホストマシンのＩＰアドレス３１３と、ホストマシン仮想マシン最大搭載台数３１４と、現在の仮想マシン搭載台数３１５との各項目情報とから構成され、例えば、ホストＩＤ「００１」の名称「ＵＶＷ」のホストが、ホストＩＤ「１７２．１６．０．１」、最大搭載台数が「２０」台、搭載数が「１０」と登録されている。これらの情報に基づき仮想マシン作成処理部２０４では、検疫が終了した仮想マシンを検疫ネットワークから業務ネットワークに移動させる際、搭載台数が最も少ないホストを選択し、ホスト間の移動を行うことができる。前記テーブル２０７～２０９に格納された前述の情報は、仮想環境管理コンピュータ１１４に予め登録された管理情報から必要な情報を抽出して格納したものである。

【００２５】

［動作］

次に上述のように構成された仮想マシンセキュリティ管理システムが適用されるコンピュータシステムの動作を図４以降のフローを参照して説明する。

［新規仮想マシン生成時動作］

まず、本実施形態によるコンピュータシステムは、仮想マシンを新規に生成するため、仮想マシンを作成したいユーザが業務ネットワーク１２０を経由して仮想マシンセキュリティ管理コンピュータ１０１に作成の依頼を出した場合、図４に示す如く、依頼を受けた仮想マシンセキュリティ管理コンピュータ１０１のメッセージ解析部２０３がメッセージマスタテーブル２０７の対策処理ＩＤ（ユーザ要求「３」）を参照してメッセージ内容がユーザからの新規作成要求であるか否かの判断を行うステップ４０１と、該ステップ４０１においてユーザからの仮想マシン新規作成依頼と判定したとき、仮想マシン作成処理部２０４へ新規仮想マシン作成依頼を行うステップ４０２と、前記ステップ４０１においてユーザからの仮想マシン新規作成依頼でないと判定したとき、ウィルス感染を検知したことによる要求か判定するステップ４０３を実行する。

【００２６】

前記ステップ４０２により新規仮想マシン作成依頼を受けた仮想マシン作成処理部２０４は、図５に示す如く、検疫環境である仮想化サーバ１１８に仮想マシン１１９をテンプレートを参照して作成するステップ５０１と、該作成した仮想マシン１１９を生成したテンプレートが検疫済みか否かを仮想マシンマスタテーブル２０８の検疫フラグを参照して判定するステップ５０２と、該ステップ５０２において検疫済みと判定したとき（検疫フラグが「１」と判定したとき）、セキュリティパッチ未適用による処理であるか否かをメッセージマスタテーブル２０７の対策処理ＩＤを参照して判定するステップ５０３と、（本処理では新規作成のため）該ステップ５０３によりセキュリティパッチ未適用による処理でないと判定し、ホストマシンマスタテーブル２０９の搭載数３１５等を参照して実運用環境セグメント（仮想化サーバ１０７）内で仮想マシンの搭載台数が最も少ないホスト（仮想化サーバ１０７）を選定するステップ５０７と、前記ステップ５０１で仮想化サーバ１１８に作成した仮想マシンを仮想化サーバ１０７に移動するステップ５０８とを実行することによって、テンプレートが検疫済みの仮想マシンの新規作成を行うことができる。尚、前記ステップ５０７及び後述するステップ５０５によるホスト（仮想化サーバ）の選択は、搭載台数に限られるものではなく、例えば（搭載台数／最大搭載台数）の値（搭載台数率）が最も小さいホストを選択しても良い。

【００２７】

［ウィルス感染時処理］

また本実施形態による仮想マシンセキュリティ管理システムが適用されるコンピュータシステムは、図４に示したステップ４０１によりメッセージがユーザ要求でないと判定したとき、ウィスルス感染時の処理であるか否かをメッセージマスタテーブル２０７の対策処理ＩＤを参照して判定するステップ４０３と、（ここではウィルス感染警告「１」のため）該ステップ４０３においてウィルス感染と判定し、仮想マシン削除処理部２０５へ感染した仮想マシンの削除を依頼するステップ４０４と、該ステップ４０４に続き、前述の新規作成と同様に仮想マシン作成処理部２０４へ新規仮想マシン作成依頼を発するステップ４０５とを実行する。

【００２８】

このステップ４０５により新規仮想マシン作成依頼を受けた仮想マシン作成処理部２０４は、前述の新規作成と同様に、図５に示した検疫環境に仮想マシンマスタテーブル２０８に登録した作成元テンプレートを参照し、前記ステップ４０４により削除した仮想マシンと同一のテンプレートにより新規仮想マシンを生成するステップ５０１－テンプレートが検疫済みか判定するステップ５０２－パッチ未適用であるか否かを判定するステップ５０３を経てステップ５０７及び５０８により新規な仮想マシンを実運用環境へ移行する様に動作することにより、感染した仮想マシンを削除し、削除した仮想マシンと同一のテンプレートにより新たに仮想マシンを作成することができる。

【００２９】

［実運用環境でパッチ未適用検出時処理］

更に本仮想マシンセキュリティ管理システムが適用されるコンピュータシステムは、図４に示したステップ４０１によりメッセージがユーザ要求でないと判定し、ウィルス感染時の処理であるか否かをメッセージマスタテーブル２０７の対策処理ＩＤを参照して判定するステップ４０３においてウィルス感染時以外の処理（パッチ未適用メッセージ「２」）と判定したとき、仮想マシン作成処理部２０４へ新規仮想マシン作成依頼を発するステップ４０６を実行する。

【００３０】

このステップ４０６により新規仮想マシン作成依頼を受けた仮想マシン作成処理部２０４は、図５に示した検疫環境に仮想マシンマスタテーブル２０８に登録した作成元テンプレートを参照し、通知が発せられた対象の仮想マシンと同一のテンプレートにより新規仮想マシンを生成するステップ５０１と、テンプレートが検疫済みか判定するステップ５０２を実行する。

【００３１】

このステップ５０２において仮想マシン作成処理部２０４が仮想マシンマスタテーブル２０８を参照してメッセージが発せられた仮想マシンの検疫フラグを確認し、例えばＩＤ「０００１」の仮想マシン「ＡＢＣ」の如く、未検疫のとき、図５に示す如く、ウィルス対策ソフトウェア１０６とパッチ管理ソフトウェア１０４による検疫を図示しない検疫システムに依頼するステップ５０９と、該ステップ５０９による検疫が合格したか否かを判定するステップ５１０と、該ステップ５１０において検疫に合格しないと判定したとき、テンプレートに異常があるとして管理者ユーザに仮想マシンが作成できないことを通知するステップ５１１を実行して処理を終了する。

【００３２】

前記ステップ５１０において検疫に合格したと判定したとき、本システムは、セキュリティパッチ未適用の処理であるかをメッセージマスタテーブル２０７を参照して判定するステップ５０３を実行し、本例においてはセキュリティパッチ未適用の処理のため、ステップ５０４による該当の仮想マシンの削除と、ステップ５０５による実運用環境セグメント（仮想化サーバ）内で仮想マシンの搭載台数が最も少ないホスト（仮想化サーバ１０７）を選定し、ステップ５０６により選定したホストに検疫環境下の仮想マシンを移動する処理を実行することによって、パッチ未適用の警告の際にも検疫済みの新たな仮想マシンを生成することができる。

【００３３】

［その他の処理］

更に本仮想マシンセキュリティ管理システムが適用されるコンピュータシステムは、図４に示したステップ４０１によりメッセージがユーザ要求でないと判定し、ウィルス感染時の処理であるか否かをメッセージマスタテーブル２０７の対策処理ＩＤを参照して判定するステップ４０３においてウィルス感染時以外の処理（その他メッセージ「４」）と判定したとき、仮想マシン作成処理部２０４へ新規仮想マシン作成依頼を発するステップ４０６を実行する。

【００３４】

このステップ４０６により新規仮想マシン作成依頼を受けた仮想マシン作成処理部２０４は、図５に示した検疫環境に仮想マシンマスタテーブル２０８に登録した作成元テンプレートを参照し、通知が発せられた対象の仮想マシンと同一のテンプレートにより新規仮想マシンを生成するステップ５０１と、テンプレートが検疫済みか判定するステップ５０２を実行する。

【００３５】

このステップ５０２において仮想マシン作成処理部２０４が仮想マシンマスタテーブル２０８を参照してメッセージが発せられた仮想マシンの検疫フラグを確認し、例えばＩＤ「０００１」の仮想マシン「ＡＢＣ」の如く、未検疫のとき、図５に示す如く、ウィルス対策ソフトウェア１０６とパッチ管理ソフトウェア１０４による検疫を図示しない検疫システムに依頼するステップ５０９と、該ステップ５０９による検疫が合格したか否かを判定するステップ５１０と、該ステップ５１０において検疫に合格しないと判定したとき、管理者ユーザに仮想マシンが作成できないことを通知するステップ５１１を実行して処理を終了する。

【００３６】

前記ステップ５１０において検疫に合格したと判定したとき、本システムは、セキュリティパッチ未適用の処理であるかをメッセージマスタテーブル２０７を参照して判定するステップ５０３を実行し、本例においてはセキュリティパッチ未適用の処理でないため、ステップ５０７及びステップ５０８によるステップ５０１により仮想化サーバ１１８に生成した仮想マシンを仮想化サーバ１１８に移動する処理を実行することによって、そのたのメッセージの場合においても検疫済みの新たな仮想マシンを生成することができる。

【００３７】

この様に本実施形態による仮想マシンセキュリティ管理方法を適用した仮想マシンセキュリティ管理システムは、ユーザ要求又はウィルス感染検知又はセキュリティパッチ未適

用によるメッセージが発せられたとき、検疫用に準備した仮想化サーバ１１８に仮想マシンを生成し、この生成した仮想マシンの元となるテンプレートが検疫済みか否かを判定し、検疫に合格した仮想マシンを検疫用環境の仮想化サーバ１１８から実稼動環境の仮想化サーバ１０７に移動することによって、ウィルス感染がなく且つセキュリティパッチの当てられた仮想マシンを生成することができる。

【図面の簡単な説明】

【００３８】

【図１】本発明の一実施形態による仮想マシンセキュリティ管理システムを適用したコンピュータシステムの全体構成図。

【図２】本実施形態による仮想マシンセキュリティ管理システムの構成を示す図。

【図３】本実施形態による各種データテーブルの構成を説明するための図。

【図４】本実施形態によるメッセージ解析部の動作フローチャート図。

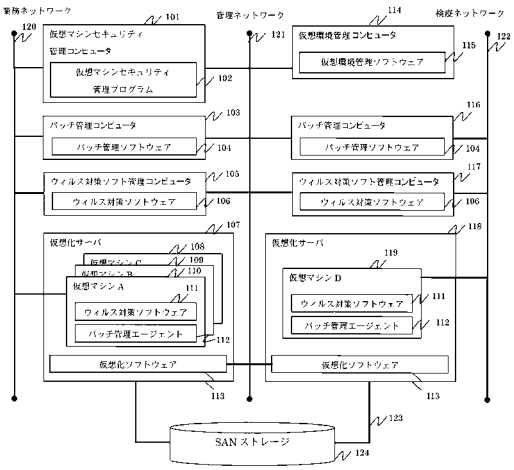
【図５】本実施形態による仮想マシン作成処理部の動作フローチャート図。

【符号の説明】

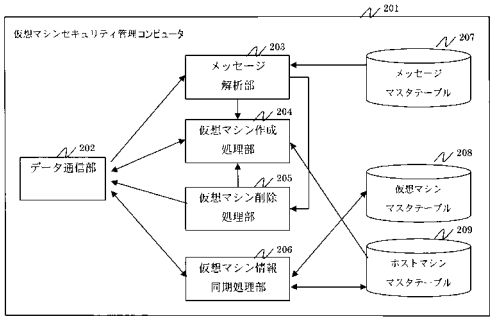
【００３９】

１０１：仮想マシンセキュリティ管理コンピュータ、１０２：仮想マシンセキュリティ管理プログラム、１０３：パッチ管理コンピュータ、１０４：パッチ管理ソフトウェア、１０５：ウィルス対策ソフト管理コンピュータ、１０６：ウィルス対策ソフトウェア、１０７：仮想化サーバ、１０８～１１０：仮想マシン、１１１：ウィルス対策ソフトウェア、１１２：パッチ管理エージェント、１１３：仮想化ソフトウェア、１１４：仮想環境管理コンピュータ、１１５：仮想環境管理ソフトウェア、１１６：パッチ管理コンピュータ、１１７：ウィルス対策ソフト管理コンピュータ、１１８：仮想化サーバ、１１９：仮想マシン、１２０：業務ネットワーク、１２１：管理ネットワーク、１２２：検疫ネットワーク、１２４：ＳＡＮストレージ、２０２：データ通信部、２０３：メッセージ解析部、２０４：仮想マシン作成処理部、２０５：仮想マシン削除処理部、２０６：仮想マシン情報同期処理部、２０７：メッセージマスタテーブル、２０８：仮想マシンマスタテーブル、２０９：ホストマシンマスタテーブル。

【図１】



【図２】



【図３】

(A) メッセージ情報テーブル

ID	メッセージ名称	対策処理ID
0001	ウィルス感染警告	1
0002	パッチ未適用警告	2
0003	ユーザ要求	3
0004	その他メッセージ	4

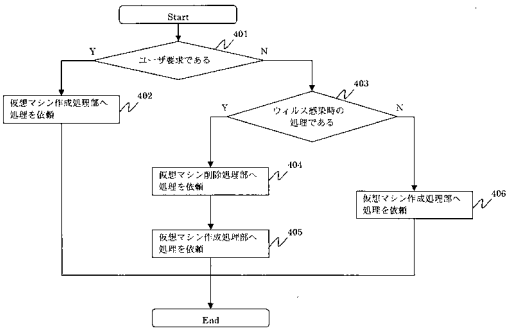
(B) 仮想マシンマスタテーブル

ID	仮想マシン名称	仮想マシンIP	ホストID	テンプレートフラグ	作成元テンプレート	検疫フラグ
0001	ABC	192.168.0.1	0001	1	−	0
0002	DEF	192.168.0.2	0001	0	ABC	1
0003	GHI	192.168.0.3	0002	0	ABC	1

(C) ホストマシンマスタテーブル

ID	ホスト名称	ホストIP	最大搭載台数	搭載数
0001	UVW	172.16.0.1	20	10
0002	XYZ	172.16.0.2	20	5

【図４】



【図５】