(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4145582号
(P4145582)
(45)発行日　平成20年9月3日(2008.9.3)　(24)登録日　平成20年6月27日(2008.6.27)

(51)Int.Cl.　F I
G06F 21/22 (2006.01)　G06F 9/06 66ON

請求項の数 2 (全 13 頁)

(21)出願番号　特願2002-190707(P2002-190707)
(22)出願日　平成14年6月28日(2002.6.28)
(65)公開番号　特開2004-38273(P2004-38273A)
(43)公開日　平成16年2月5日(2004.2.5)
審査請求日　平成17年4月20日(2005.4.20)

特許法第３０条第１項適用　２００２年５月６日　社団法人電子情報通信学会発行の「電子情報通信学会技術研究報告　信学技報　Ｖｏｌ．１０２　Ｎｏ．４５」に発表

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(73)特許権者　500030530
森井　昌克
徳島県徳島市助任本町３－２６
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(72)発明者　竹森　敬祐
埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内

最終頁に続く

(54)【発明の名称】コンピュータウィルス検査装置およびメールゲートウェイシステム

(57)【特許請求の範囲】
【請求項１】
実ホストのメモリ上に仮想ホストを構築するホストエミュレータと、
入力された被検査ファイルを前記仮想ホスト上で実行させて前記仮想ホストの動作結果を監視し、この監視結果に基づいて前記被検査ファイルがコンピュータウィルスに感染しているか否かを判断する検査処理手段と、
検査結果を通知する結果通知手段と、を具備し、
前記仮想ホスト上の標準状態における所定ファイルの特徴値を予め求めておき、
前記検査処理手段は、前記仮想ホスト上で前記被検査ファイルを実行後、前記所定ファイルの特徴値を求め、この特徴値と前記標準状態における特徴値とを比較し、不一致の場合に前記被検査ファイルがコンピュータウィルスに感染していると判断するものであり、
前記検査処理手段は、メモリ使用量を変化させながら被検査ファイルを実行させることを特徴とするコンピュータウィルス検査装置。
【請求項２】
請求項１に記載のコンピュータウィルス検査装置と、
メールサービス利用者の端末と外部ネットワークとの間で相互に電子メールを転送するメール転送手段とから構成され、
前記メール転送手段は、転送する電子メールの添付ファイルのコンピュータウィルス検査を前記コンピュータウィルス検査装置へ依頼し、
前記コンピュータウィルス検査装置は、この検査によりコンピュータウィルスが未検知

であった場合に前記電子メールの転送を許可し、コンピュータウィルスを検知した場合には前記電子メールの少なくとも添付ファイルの転送を許可しない
ことを特徴とするメールゲートウェイシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子メールの添付ファイルなどのコンピュータウィルス検査を行うコンピュータウィルス検査装置、並びにメールゲートウェイシステムに関する。
【０００２】
【従来の技術】
近年、インターネットの普及により電子メールが広く利用されているが、電子メールの添付ファイルによりコンピュータウィルス（以下、単にウィルスと称する）が媒介され多くのコンピュータに感染しており、このことが社会問題となっている。このためにウィルス対策ベンダーから、既知ウィルスの検出用のパターンファイルが提供されている。このパターンファイルには、ウイルス特有のコード、例えば通信ポートのフックコードなどのファンクションコールと呼ばれるものが定義されている。そして、パターンファイルに定義されているコードと添付ファイルのバイナリコードを比較して一致した場合にウィルスと判断することができる。この検査手法は、スタティックヒューリスティック検査と呼ばれている。しかし、ウィルス対策ベンダーから対応済みのパターンファイルがリリースされる前に、急速に広がりをみせるウィルスが多く現れており、このような未知のウィルスへの対策が強く望まれている。
【０００３】
このような背景の中、ダイナミックヒューリスティック検査と呼ばれる手法によって未知のウィルスを検知する技術が、例えば「竹内大輔，千石靖，服部進実，“仮想マシンを用いた実行形式型ウィルスの検出”，コンピュータセキュリティシンポジウム ２００１，pp.179-184，0ct.2001」に記載されている。ダイナミックヒューリスティック検査とは、コンピュータシステムのメモリ上でウィルスの疑いのあるファイルを仮想的に実行して、ウィルス特有のファンクションコールが有った場合にウィルスと判断する手法である。この手法を用いて、ユーザのコンピュータのメモリ上で電子メールの添付ファイルを仮想的に実行すれば、パターンファイルにない未知のウィルスを検出することが可能である。
【０００４】
【発明が解決しようとする課題】
しかし、上述した従来のダイナミックヒューリスティック検査による手法では、予想される全てのファンクションコールに予め対応しておく必要があるために、容易にウィルス検査を行うことができないという問題がある。
【０００５】
さらに、未対応のファンクションコールがあったり、あるいはファンクションコール定義ファイルの作成ミスがあると、検査に用いるコンピュータ自体がウィルスに感染してしまうという問題もある。
【０００６】
ここで、検査用のコンピュータ（以下、実ホストと称する）へのウィルス感染を防ぐために、ホストエミュレータを用いて実ホストのメモリ上に仮想ホストを構築し、この仮想ホスト上で疑わしいファイルを実行して検査することが考えられる。ホストエミュレータは、例えば「ＶＭｗａｒｅ（登録商標）」と呼ばれるコンピュータプログラムを利用して実現することが可能である。これにより実ホストのメモリ上に仮想ホストを構築し、該仮想ホスト上で電子メールの添付ファイルを実行すれば、仮想ホストにウィルスが感染しても、実ホストへのウィルス感染を防ぐことが可能である。
【０００７】
本発明は、このような事情を考慮してなされたもので、その目的は、仮想ホストを構築し、該仮想ホスト上で被検査ファイルを実行することにより実ホストへのウィルス感染を

防止し、且つ容易にウィルス検査を行うことができるコンピュータウィルス検査装置を提供することにある。

【０００８】

また、本発明は、そのコンピュータウィルス検査装置を備え、電子メールの添付ファイルを媒体として感染するコンピュータウィルスの拡散を防止することができるメールゲートウェイシステムを提供することも目的とする。

【００１０】

【課題を解決するための手段】

上記の課題を解決するために、本発明に係るコンピュータウィルス検査装置は、実ホストのメモリ上に仮想ホストを構築するホストエミュレータと、入力された被検査ファイルを前記仮想ホスト上で実行させて前記仮想ホストの動作結果を監視し、この監視結果に基づいて前記被検査ファイルがコンピュータウィルスに感染しているか否かを判断する検査処理手段と、検査結果を通知する結果通知手段と、を具備し、前記仮想ホスト上の標準状態における所定ファイルの特徴値を予め求めておき、前記検査処理手段は、前記仮想ホスト上で前記被検査ファイルを実行後、前記所定ファイルの特徴値を求め、この特徴値と前記標準状態における特徴値とを比較し、不一致の場合に前記被検査ファイルがコンピュータウィルスに感染していると判断することを特徴とする。

この発明によれば、ホストエミュレータにより仮想ホストを構築し、検査処理手段が該仮想ホスト上で被検査ファイルを実行することにより実ホストへのウィルス感染を防止することができる。さらに、検査処理手段が仮想ホストの動作結果に基づいて被検査ファイルがコンピュータウィルスに感染しているか否かを判断するので、容易にウィルス検査を行うことができる。この発明によれば、検査処理手段が仮想ホストの動作結果として所定ファイルの内容の変化があったか否かを監視するので、所定ファイルを改ざんするコンピュータウィルスを検知することができる。

【００１１】

本発明に係るコンピュータウィルス検査装置においては、前記検査処理手段が特徴値を求めるファイルは、過去にコンピュータウィルスによって改ざんが行われたファイルと同じファイル拡張子を有するファイル、又は、コンピュータウィルスによる改ざんによってコンピュータシステム上の不具合が引き起こされる虞のあるファイルに限定されていることを特徴とする。

【００１２】

本発明に係るコンピュータウィルス検査装置においては、前記検査処理手段は、複数のアプリケーションプログラムを起動させた状態で被検査ファイルの実行を行うことを特徴とする。

【００１３】

本発明に係るコンピュータウィルス検査装置においては、前記検査処理手段は、メモリ使用量を変化させながら被検査ファイルを実行させることを特徴とする。

【００１４】

本発明に係るコンピュータウィルス検査装置においては、前記検査処理手段は、前記被検査ファイルが圧縮されている場合には、該圧縮の解凍を行いながら検査を行うことを特徴とする。

この発明によれば、検査処理手段が圧縮解凍するので、圧縮済みのファイルであっても検査可能である。

【００１５】

本発明に係るコンピュータウィルス検査装置においては、前記検査処理手段は、パターンマッチング検査機能とスタティックヒューリスティック検査機能を有し、これら検査によってコンピュータウィルスが未検知であった前記被検査ファイルのみを、前記仮想ホスト上で実行させて検査することを特徴とする。

この発明によれば、仮想ホストを用いた検査の対象となる被検査ファイルの数が削減されるので、能率よくウィルス検査を実施することができ、ウィルス検査全体の処理速度を

向上させることができる。

【００１６】

本発明に係るコンピュータウィルス検査装置においては、前記検査処理手段は、前記仮想ホスト上で実行させて検査した結果、コンピュータウィルスを検知した場合に、当該コンピュータウィルスを分析して特徴を抽出し、この特徴をパターンマッチング検査用またはスタティックヒューリスティック検査用のパターンファイルに反映させることを特徴とする。

この発明によれば、仮想ホストを用いた検査によって検知された未知のウィルスの特徴が、パターンマッチング検査用またはスタティックヒューリスティック検査用のパターンファイルに反映されるので、ウィルス検査の精度を効率よく向上させることができる。

【００１７】

本発明に係るコンピュータウィルス検査装置においては、前記結果通知手段は、前記被検査ファイルがコンピュータウィルス感染済みであった場合、該被検査ファイル実行時の動作状況または検査内容を結果通知用電子メールに記載して出力することを特徴とする。

この発明によれば、検知したコンピュータウィルスの内容を電子メールにより即時に通知することが可能となり、ウィルス拡散防止に寄与することができる。

【００１８】

本発明に係るコンピュータウィルス検査装置においては、前記結果通知手段は、前記結果通知用電子メールに電子署名を施すことを特徴とする。

この発明によれば、電子署名により検査結果の内容の正当性が保証される。

【００１９】

上記の課題を解決するために、本発明に係るメールゲートウェイシステムは、前述のコンピュータウィルス検査装置と、メールサービス利用者の端末と外部ネットワークとの間で相互に電子メールを転送するメール転送手段とから構成され、前記メール転送手段は、転送する電子メールの添付ファイルのコンピュータウィルス検査を前記コンピュータウィルス検査装置へ依頼し、前記コンピュータウィルス検査装置は、この検査によりコンピュータウィルスが未検知であった場合に前記電子メールの転送を許可し、コンピュータウィルスを検知した場合には前記電子メールの少なくとも添付ファイルの転送を許可しないことを特徴としている。

この発明によれば、コンピュータウィルス検査装置が、メール転送手段によって転送される電子メールの添付ファイルの検査結果に基づいて該電子メールの転送許可を行うので、電子メールの添付ファイルを媒体として感染するコンピュータウィルスの拡散を防止することができる。

【００２０】

本発明に係るメールゲートウェイシステムにおいては、前記コンピュータウィルス検査装置は、少なくともコンピュータウィルスを検知した前記添付ファイルを一括保管及び管理することを特徴とする。

この発明によれば、コンピュータウィルスに感染済みの添付ファイルが隔離されるので、利用者がコンピュータウィルスに感染済み添付ファイルを誤って実行してしまうことを未然に防ぐことができる。

【００２１】

本発明に係るメールゲートウェイシステムにおいては、前記コンピュータウィルス検査装置は、前記保管中の添付ファイルへアクセスするための通信アドレスを前記端末に通知することを特徴とする。

この発明によれば、保管中の添付ファイルへのアクセス用通信アドレスが通知されるので、利用者は必要に応じて保管中の添付ファイルへアクセスすることができる。これにより、利用者の不用意な添付ファイルの実行を抑制し、コンピュータウィルスの感染を防止することができる。

【００２３】

上記の課題を解決するために、本発明に係るコンピュータプログラムは、実ホストのメ

モリ上に仮想ホストを構築する処理と、前記仮想ホスト上の標準状態における所定ファイルの特徴値を予め求める処理と、入力された被検査ファイルを前記仮想ホスト上で実行させる処理と、前記仮想ホストの動作結果を監視する処理と、この監視結果に基づいて、前記仮想ホスト上で前記被検査ファイルを実行後、前記所定ファイルの特徴値を求め、この特徴値と前記標準状態における特徴値とを比較し、不一致の場合に前記被検査ファイルがコンピュータウィルスに感染していると判断する処理と、検査結果を通知する処理とをコンピュータに実行させることを特徴としている。

この発明によれば、前記各処理をコンピュータにより実行することが可能となる。これにより、前述のコンピュータウィルス検査装置がコンピュータを利用して実現できるようになる。

【００２４】

【発明の実施の形態】

以下、図面を参照し、本発明の一実施形態について説明する。

図１は、本発明の一実施形態によるウィルス検査サーバ（コンピュータウィルス検査装置）１の構成を示すブロック図である。ウィルス検査サーバ１は、ＣＰＵおよびメモリから構成される処理部と、該ＣＰＵで実行されるプログラムや各種データを記憶する記憶部（メモリやハードディスク等）などからなるコンピュータ（実ホスト）により構成される。図１には、該ＣＰＵが記憶部に記憶されているプログラムを実行して実現する機能を展開したブロック構成のうち、便宜上、本発明に係る構成部分を示している。

【００２５】

図１において、ウィルス検査サーバ１は、実ホスト上で実現される検査処理部１１と、実ホスト上で実現されるホストエミュレータ２０によって実ホストのメモリ上に構築された仮想ホストＡ＿２１，仮想ホストＢ＿２２とを有する。検査処理部１１は、実ホスト上で検査処理部１１の機能を実現するためのプログラムを実行することにより実現される。ホストエミュレータ２０は、例えば「ＶＭｗａｒｅ（登録商標）」と呼ばれるコンピュータプログラムを実ホスト上で実行することにより実現される。

【００２６】

仮想ホストＡ＿２１，Ｂ＿２２は、ホストエミュレータ２０により、それぞれ異なるオペレーティングシステム（ＯＳ）を実行するものとして構築される。例えば、「Windows（登録商標）系のＯＳ」や「Linux」などのＯＳである。なお、本実施形態においては、仮想ホストとして異なるＯＳを実行する２つを設けるようにしたが、仮想ホストは１つであっても、あるいは３つ以上であってもよい。

【００２７】

検査処理部１１は、入力された被検査ファイルを仮想ホストＡ＿２１，Ｂ＿２２上でそれぞれ実行させる。そして、各仮想ホストＡ＿２１，Ｂ＿２２の動作結果を監視し、この監視結果に基づいて被検査ファイルがウィルスに感染しているか否かを判断する。以下に、このウィルス検査方法について説明する。

【００２８】

検査処理部１１が監視対象とする仮想ホストの動作結果としては、各種考えられるが、ここでは２つの例を説明する。

（１）メール送信の監視によりウィルスを検知する方法

この方法では、各仮想ホストＡ＿２１，Ｂ＿２２に電子メールの送信プログラムをインストールし、この送信プログラムを実行可能なようにしておく。また、電子メールの宛先に使用可能なように、ダミーの電子メールアドレスを設定しておく。

次いで、検査処理部１１は、被検査ファイルを仮想ホストＡ＿２１，Ｂ＿２２上でそれぞれ実行させて、仮想ホストＡ＿２１，Ｂ＿２２が電子メールを送信するか否かを監視する。

次いで、検査処理部１１は、電子メールの送信を行った仮想ホストがあった場合に、被検査ファイルがウィルスに感染していると判断する。

この方法によれば、電子メールの添付ファイルを被検査ファイルとすることにより、該添

付ファイルを媒体として感染を拡散させるウィルスを検知することができる。
【００２９】
（２）ファイルの改ざんの監視によりウィルスを検知する方法
この方法では、各仮想ホストＡ＿２１，Ｂ＿２２上の標準状態におけるファイルの特徴値を予め求めておく。この特徴値としてはハッシュ値が利用可能である。
次いで、検査処理部１１は、被検査ファイルを仮想ホストＡ＿２１，Ｂ＿２２上でそれぞれ実行させる。
次いで、検査処理部１１は、各仮想ホストＡ＿２１，Ｂ＿２２上のファイルの特徴値を求め、この特徴値と標準状態における特徴値を比較する。
次いで、検査処理部１１は、この比較の結果が不一致の場合に、被検査ファイルがウィルスに感染していると判断する。
【００３０】
但し、特徴値を求めるファイルは、過去にウィルスによって改ざんが行われたファイルのと同じファイル拡張子を有するものに限定する。あるいは、改ざんによってコンピュータシステム上の不具合が引き起こされる虞のあるファイルに限定する。これにより、ウィルスによるものではなく、正常な処理によって内容が変更されるファイルについては、改ざん監視対象から除外できるので、ウィルスの誤検出を防止することができる。また、全てのファイルの特徴値（ハッシュ値）を求める必要が無いので、処理速度が向上する。
【００３１】
なお、被検査ファイルがウィルスに感染していた場合、上記ウィルス検査により、仮想ホストＡ＿２１またはＢ＿２２はウィルスに感染してしまう。しかし、ホストエミュレータ２０を再起動して仮想ホストＡ＿２１，Ｂ＿２２を再構築することにより、実ホストへの影響なく、且つ短時間で検査可能な状態に復帰することができる。
【００３２】
また、検査処理部１１は、ウィルスの影響が顕在化するように、仮想ホストＡ＿２１，Ｂ＿２２上で被検査ファイルを実行する際の実行条件を変化させる。例えば、仮想ホスト上の日時やメモリ使用量を変化させながら被検査ファイルを実行させる。あるいは複数のアプリケーションプログラムを起動させた状態で被検査ファイルの実行を行う。これにより、特定の実行条件下（例えば特定の日時）でのみ発病するウィルスであっても検知することができる。
【００３３】
また、検査処理部１１は、被検査ファイルが圧縮されている場合には、該圧縮の解凍を行いながら検査を行う。これにより、例えば電子メールの添付ファイルは圧縮して転送されることがしばしばなされるが、このように圧縮ファイルによって媒介される場合においてもウィルスの検知を行うことができる。
【００３４】
次に、上述した図１のウィルス検査サーバ１を備えたメールゲートウェイシステムの実施例を説明する。図２、図３はメールゲートウェイシステム３０の動作を説明するためのシーケンス図である。図２、図３に示すメールゲートウェイシステム３０は、ウィルス検査サーバ１とメールサーバ３１（メール転送手段）から構成される。メールサーバ３１は、メールサービス利用者の端末４０と外部ネットワークとの間で相互に電子メール（以下、単にメールと称する）を転送する機能を有する。但し、この転送の際に、メールサーバ３１は、転送するメールの添付ファイルのウィルス検査をウィルス検査サーバ１へ依頼し、この検査結果に基づくメールの転送可否判断の結果に従って動作する。
【００３５】
初めに、図２を参照して、送信者が端末４０により添付ファイル付きメールを送信した際のウィルス検査に係る動作を説明する。先ず、送信者が端末４０により添付ファイル付きメール１０１を送信する（ステップＳ１）。メールサーバ３１は、添付ファイル付きメール１０１を受け取ると、この添付ファイル付きメール１０１をウィルス検査サーバ１へ提供してウィルス検査を依頼する（ステップＳ２）。

【００３６】
次いで、ウィルス検査サーバ１は、添付ファイル付きメール１０１の添付ファイルを被検査ファイルとしてウィルス検査を実行し、この検査結果をメールサーバ３１及び端末４０へ通知する（ステップＳ３）。この通知が検査正常であり、添付ファイルがウィルスに感染していない場合に、メールサーバ３１は、添付ファイル付きメール１０１を外部ネットワークへ転送する（ステップＳ４）。
【００３７】
これにより、添付ファイルを媒体として感染を拡散させるウィルスが外部ネットワークへ流出することを防止することができる。
【００３８】
次に、図３を参照して、メールサーバ３１が外部ネットワークから添付ファイル付きメールを受信した際のウィルス検査に係る動作を説明する。先ず、メールサーバ３１は、外部ネットワークから添付ファイル付きメール１１０を受信すると（ステップＳ１１）、添付ファイル付きメール１１０をウィルス検査サーバ１へ提供してウィルス検査を依頼する（ステップＳ１２）。
【００３９】
次いで、ウィルス検査サーバ１は、添付ファイル付きメール１１１の添付ファイルを被検査ファイルとしてウィルス検査を実行し、この検査結果をメールサーバ３１へ通知する（ステップＳ１３）。ここで、ウィルス検査サーバ１は添付ファイルを保存しておく。
【００４０】
次いで、メールサーバ３１は、ウィルス検査結果の通知内容を記載した検査結果メール１２０を作成して受信者の端末４０へ送信する（ステップＳ１４）。この検査結果メール１２０には、図５または図６に示すように、添付ファイル付きメール１１０のメールヘッダ１１２及び本文１１３と、添付ファイルの動作検査結果１２１と、添付ファイル取得用ＵＲＬ（Uniform Resource Locator）１２２とが記載される。また、図６に示すように、さらに電子署名１２３を記載するようにしてもよい。添付ファイルの動作検査結果１２１及び添付ファイル取得用ＵＲＬ１２２及び電子署名１２３については、ウィルス検査サーバ１が作成してメールサーバ３１へ提供する。
【００４１】
添付ファイルの動作検査結果１２１は、ウィルス検査サーバ１で添付ファイルを実行した時の動作状況や検査内容を示すものである。動作検査結果１２１には、添付ファイルがウィルス感染済みであると判断した場合に、添付ファイル実行時にウィルスの挙動としてどのような動作が行われたのか、またウィルスを検知した検査項目や使用パターンファイル名などが示される。一方、添付ファイルがウィルス未感染であると判断した場合には、どの検査を実施したのかが示される。なお、検査項目の詳細（パターンファイルを使用する検査等）については後述する。
【００４２】
添付ファイル取得用ＵＲＬ１２２は、ウィルス検査サーバ１に保存してある添付ファイルを取得するためのアドレスである。受信者は、端末４０により、この添付ファイル取得用ＵＲＬ１２２を使用してウィルス検査サーバ１にアクセスし、該当する添付ファイルを取得することができる（ステップＳ１５）。
【００４３】
電子署名１２３は、検査結果メール１２０の正当性を証明するためのものである。ウィルス検査サーバ１は、この電子署名１２３によって当該検査結果メール１２０の内容を保証する。
【００４４】
これにより、添付ファイルを媒体として感染を拡散させるウィルスが外部ネットワークから流入することを防止することができる。
【００４５】
次に、図４を参照して、上述した図２，図３のメールゲートウェイシステム３０における

ウィルス検査サーバ１の動作を説明する。図４は、メールゲートウェイシステム３０において、図１の検査処理部１１が行うウィルス検査処理の流れを示すフローチャートである。この図４に示すウィルス検査は、パターンマッチング検査とスタティックヒューリスティック検査とダイナミックヒューリスティック検査の３つの検査項目からなる。

【００４６】

パターンマッチング検査とは、メールヘッダなどから明らかにウィルスであると判定できる要素をパターンマッチングにより検出して、ウィルスの検知を行うものである。このパターンマッチング検査は従来から行われており、本実施形態においても従前の方法で行う。また、スタティックヒューリスティック検査についても、従前の方法で行う。これらパターンマッチング検査及びスタティックヒューリスティック検査で用いる各パターンファイルは、予めウィルス検査サーバ１に設定されている。

【００４７】

ダイナミックヒューリスティック検査については、上記図１を参照して説明した本実施形態のウィルス検査方法（メール送信監視によるウィルス検知、又はファイル改ざん監視によるウィルス検知）を使用して行う。

【００４８】

図４において、検査処理部１１は、メールサーバ３１から添付ファイル付きメールを受け取ると、添付ファイルを取り出して保存する（ステップＳ２１）。次いで、検査処理部１１は、該添付ファイルに対してパターンマッチング検査を実施する（ステップＳ２２）。この検査の結果、ウィルスを検知し、ウィルス感染済みと判断した場合にはステップＳ３４へ進む（ステップＳ２３）。一方、ウィルスを検知せず、ウィルス未感染と判断した場合には、さらにスタティックヒューリスティック検査を実施する（ステップＳ２４）。

【００４９】

この検査の結果、ウィルスを検知し、ウィルス感染済みと判断した場合にはステップＳ３４へ進む（ステップＳ２５）。一方、ウィルスを検知せず、ウィルス未感染と判断した場合には、さらにダイナミックヒューリスティック検査を実施する（ステップＳ２６）。

【００５０】

この検査の結果、ウィルスを検知し、ウィルス感染済みと判断した場合にはステップＳ３０へ進む（ステップＳ２７）。一方、ウィルスを検知せず、ウィルス未感染と判断した場合には、当該添付メールが送信メールに添付されたものか否かを判断する（ステップＳ２８）。この判断の結果、送信メールであった場合に、検査処理部１１は、メールサーバ３１へウィルス検査の結果が正常である旨を通知し、メールの送信を許可する（ステップＳ２９）。一方、送信メールでなかった場合にはステップＳ３４へ進む。

【００５１】

ステップＳ３０では、検査処理部１１は、今回のダイナミックヒューリスティック検査で検知したウィルスが各パターンファイルに含まれていない未知のものであるので、当該ウィルスを分析しその特徴を抽出する。次いで、抽出した特徴をフィードバックすることにより各パターンファイルを更新する（ステップＳ３１）。例えば、メールヘッダ中の件名（subject）を抽出して、パターンマッチング検査用のパターンファイルに追加する。また、当該添付ファイルのデータに基づいてスタティックヒューリスティック検査用のパターンファイルを更新する。

【００５２】

次いで、ステップＳ３２で、当該添付ファイルが送信メールに添付されたものか否かを判断し、この判断の結果、送信メールであった場合に、検査処理部１１は、メールサーバ３１へウィルス検査の結果が異常である旨を通知してメールの送信を中止させ、この旨を送信者の端末４０へ通知する（ステップＳ３３）。一方、送信メールでなかった場合にはステップＳ３４へ進む。

【００５３】

ステップＳ３４では、検査処理部１１は、添付ファイルがウィルスに感染済みである旨をメールサーバ３１へ通知して、検査結果メールにより受信者の端末４０へ通知させる（ス

テップＳ３４）。

【００５４】

上述したメールゲートウェイシステム３０の実施例では、先ず、パターンマッチング検査とスタティックヒューリスティック検査を実施し、これら検査でウィルスを検知できなかった添付ファイルのみに対して本実施形態のダイナミックヒューリスティック検査を実施する。これにより、仮想ホストを用いた検査（本実施形態のダイナミックヒューリスティック検査）は処理量が多く時間がかかるが、該検査対象となる添付ファイル数を削減させて、能率よくウィルス検査を実施し、ウィルス検査全体の処理速度を向上させることができる。また、ウィルス検査サーバ１にかかる負荷が軽減されるので、メールゲートウェイシステム全体の処理能力の向上を図ることも可能となる。

【００５５】

さらに、本実施形態のダイナミックヒューリスティック検査によって検知された未知のウィルスについてその特徴を抽出し、該特徴をパターンマッチング検査用またはスタティックヒューリスティック検査用のパターンファイルに反映するので、ウィルス検査の精度を効率よく向上させることができる。

【００５６】

また、本実施例では、外部ネットワークから受信した添付ファイルをウィルス検査サーバ１で一括保管及び管理し、ウィルスに感染済みの添付ファイルを利用者に直接転送しないようにしている。これにより、ウィルスに感染済みの添付ファイルを隔離し、利用者がウィルスに感染済み添付ファイルを誤って実行してしまうことを未然に防ぐことができる。なお、ウィルス検査サーバ１で一括保管及び管理する添付ファイルは、ウィルス感染済みのファイルのみとしてもよく、あるいは全ての添付ファイルであってもよい。また、ウィルス感染済みの添付ファイルについては、利用者からのアクセスに制限を設けるようにするのが、添付ファイルの誤実行によるウィルス感染の防止の点から好ましい。

【００５７】

なお、ウィルス検査サーバ１が検査結果メールを作成し、この検査結果メールをメールサーバ３１を介してメールサービス利用者の端末へ送信するようにしてもよい。

【００５８】

また、ウィルス検査サーバ１が行う各処理を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することによりウィルス検査処理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものであってもよい。

また、「コンピュータシステム」は、ＷＷＷシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、ＣＤ－ＲＯＭ等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００５９】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（ＲＡＭ）のように、一定時間プログラムを保持しているものも含むものとする。

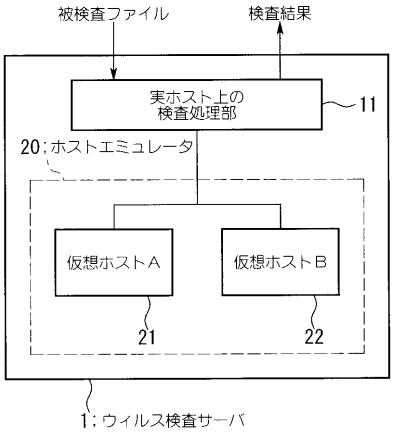
また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み

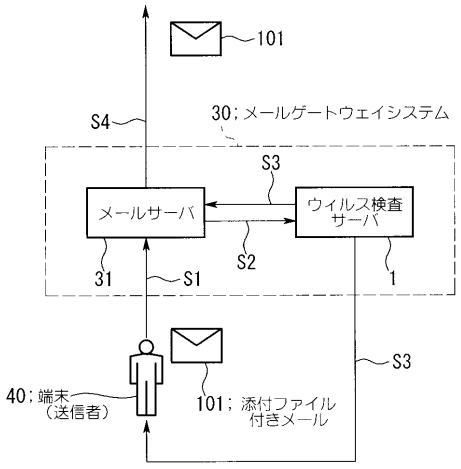
合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。
【００６０】
以上、本発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。
【００６１】
【発明の効果】
以上説明したように、本発明によれば、ホストエミュレータにより仮想ホストを構築し、該仮想ホスト上で被検査ファイルを実行することにより実ホストへのウィルス感染を防止することができる。さらに、仮想ホストの動作結果に基づいて被検査ファイルがコンピュータウィルスに感染しているか否かを判断するので、容易にウィルス検査を行うことができる。
【００６３】
本発明によれば、仮想ホストの動作結果として所定ファイルの内容の変化があったか否かを監視するので、所定ファイルを改ざんするコンピュータウィルスを検知することができる。
【００６４】
本発明によれば、実行条件を変化させて検査するので、特定の実行条件下でのみ発病するコンピュータウィルスであっても顕在化させて検知することができる。
【００６５】
本発明によれば、圧縮済みのファイルであっても検査可能である。
【００６６】
本発明によれば、仮想ホストを用いた検査の対象となる被検査ファイルの数が削減されるので、能率よくウィルス検査を実施することができ、ウィルス検査全体の処理速度を向上させることができる。
【００６７】
本発明によれば、仮想ホストを用いた検査によって検知された未知のウィルスの特徴が、パターンマッチング検査用またはスタティックヒューリスティック検査用のパターンファイルに反映されるので、ウィルス検査の精度を効率よく向上させることができる。
【００６８】
本発明によれば、検知したコンピュータウィルスの内容を電子メールにより即時に通知することが可能となり、ウィルス拡散防止に寄与することができる。
本発明によれば、電子署名により検査結果の内容の正当性が保証される。
【００６９】
本発明によれば、コンピュータウィルス検査装置が、メール転送手段によって転送される電子メールの添付ファイルの検査結果に基づいて該電子メールの転送許可を行うので、電子メールの添付ファイルを媒体として感染するコンピュータウィルスの拡散を防止することができる。
【００７０】
本発明によれば、コンピュータウィルスに感染済みの添付ファイルが隔離されるので、利用者がコンピュータウィルスに感染済み添付ファイルを誤って実行してしまうことを未然に防ぐことができる。
【００７１】
本発明によれば、保管中の添付ファイルへのアクセス用通信アドレスが通知されるので、利用者は必要に応じて保管中の添付ファイルへアクセスすることができる。これにより、利用者の不用意な添付ファイルの実行を抑制し、コンピュータウィルスの感染を防止することができる。
【図面の簡単な説明】
【図１】　本発明の一実施形態によるウィルス検査サーバ（コンピュータウィルス検査装置）１の構成を示すブロック図である。
【図２】　図１に示すウィルス検査サーバ１を備えたメールゲートウェイシステム３０の

動作を説明するための第１のシーケンス図である。
【図３】　図１に示すウィルス検査サーバ１を備えたメールゲートウェイシステム３０の動作を説明するための第２のシーケンス図である。
【図４】　メールゲートウェイシステム３０において、図１の検査処理部１１が行うウィルス検査処理の流れを示すフローチャートである。
【図５】　検査結果メールの第１の構成例を示す図である。
【図６】　検査結果メールの第２の構成例を示す図である。
【符号の説明】
１…ウィルス検査サーバ（コンピュータウィルス検査装置）、１１…検査処理部、２０…ホストエミュレータ、２１，２２…仮想ホスト、３０…メールゲートウェイシステム、３１…メールサーバ、４０…端末、１０１，１１０添付ファイル付きメール、１１１…添付ファイル、１２０，１２０ａ，１２０ｂ…検査結果メール

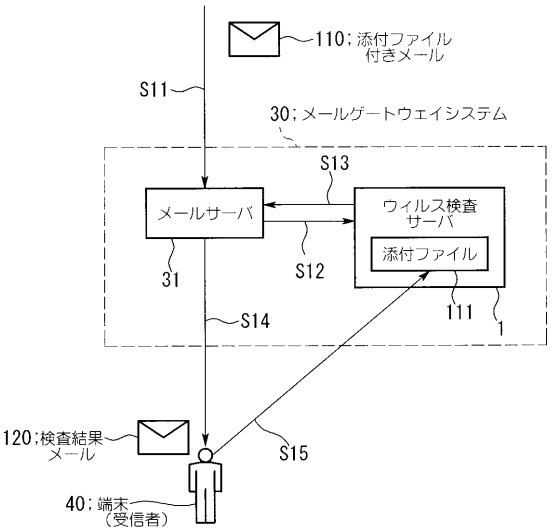
【図１】



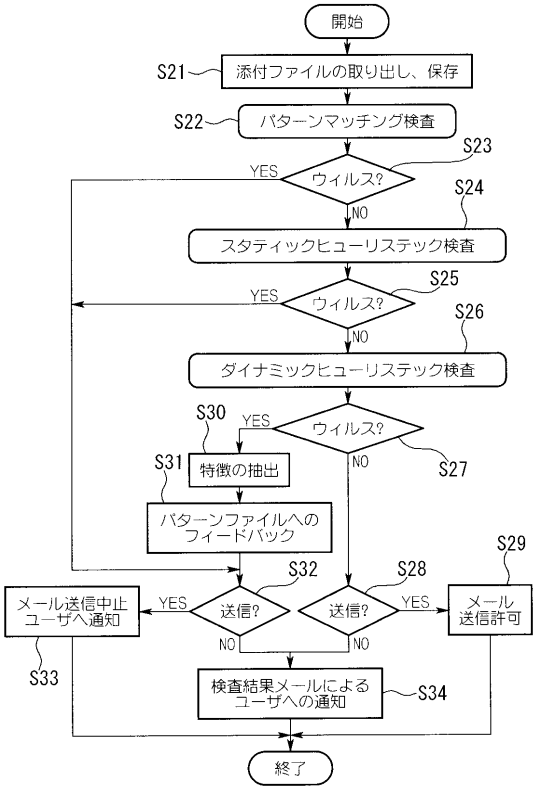
【図２】



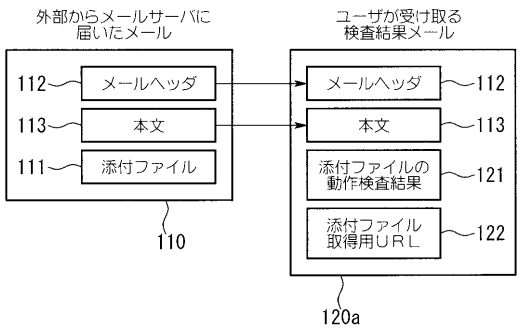
【図３】


110；添付ファイル
付きメール
S11
30；メールゲートウェイシステム
S13
メールサーバ
ウィルス検査
サーバ
添付ファイル
31
S12
111
1
S14
120；検査結果
メール
S15
40；端末
（受信者）

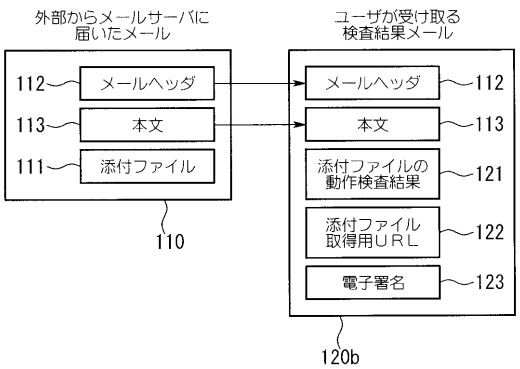
【図４】


開始
S21
添付ファイルの取り出し、保存
S22
パターンマッチング検査
S23
YES
ウィルス?
NO
S24
スタティックヒューリステック検査
YES
S25
ウィルス?
NO
S26
ダイナミックヒューリステック検査
S30
YES
ウィルス?
NO
S27
S31
特徴の抽出
パターンファイルへの
フィードバック
S29
S32
S28
メール送信中止
ユーザへ通知
YES
送信?
送信?
YES
メール
送信許可
NO
NO
S33
検査結果メールによる
ユーザへの通知
S34
終了

【図５】


外部からメールサーバに
届いたメール
ユーザが受け取る
検査結果メール
112
メールヘッダ
113
本文
111
添付ファイル
110
メールヘッダ
112
本文
113
添付ファイルの
動作検査結果
121
添付ファイル
取得用ＵＲＬ
122
120a

【図６】


外部からメールサーバに
届いたメール
ユーザが受け取る
検査結果メール
112
メールヘッダ
113
本文
111
添付ファイル
110
メールヘッダ
112
本文
113
添付ファイルの
動作検査結果
121
添付ファイル
取得用ＵＲＬ
122
電子署名
123
120b

フロントページの続き

(72)発明者　中尾　康二
埼玉県上福岡市大原２丁目１番１５号　株式会社ケイディーディーアイ研究所内
(72)発明者　森井　昌克
徳島県徳島市助任本町３２６　桑田園４０２号
(72)発明者　三宅　崇之
徳島県徳島市北矢三町２－３－５３　シルエットプリンセスA－２０２
(72)発明者　白石　善明
大阪府東大阪市新家中町１－８－９０６

審査官　宮司　卓佳

(56)参考文献　国際公開第０２／００６９２８（WO，Ａ１）
特開平０９－１７１４６０（ＪＰ，Ａ）
特開平１１－１３４１９０（ＪＰ，Ａ）
特開２００２－１８２９４２（ＪＰ，Ａ）
特開平１１－１１０２１１（ＪＰ，Ａ）
特表平１０－５０１３５４（ＪＰ，Ａ）
中島　募，メール・フィルタリング・ソフト：機密情報などをブロック，添付ファイルや暗号メールの対応も進む，日経インターネットテクノロジー，日本，日経ＢＰ社　Nikkei Business Publications,Inc.，２０００年　1月２２日，第３１号，p.120-p.127
ヒューリスティック手法詳説：シマンテックのBloodhound技術，シマンテック　ホワイトペーパー，シマンテック，２００２年　1月２５日，ＵＲＬ，http://www.symantec.com/region/jp/sarcj/reference/heuristc.pdf
渡邉利和，Ｌｉｎｕｘビジネスソフトウェア　サーバ系ディストリビューション、ＩｎｔｅｒＳｃａｎ　ＶｉｒｕｓＷａｌｌ、Ｗｅｂグループウェア、便利なツール，Ｌｉｎｕｘ　ｂｕｓｉｎｅｓｓ，日本，株式会社アスキー，２００１年　1月　8日，Vol.1，p.164-p.173

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　21/22