(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3947110号
(P3947110)
(45)発行日　平成19年7月18日(2007.7.18)　(24)登録日　平成19年4月20日(2007.4.20)

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

請求項の数 15 (全 15 頁)

(21)出願番号　特願2002-582335(P2002-582335)
(86)(22)出願日　平成14年4月9日(2002.4.9)
(65)公表番号　特表2004-531812(P2004-531812A)
(43)公表日　平成16年10月14日(2004.10.14)
(86)国際出願番号　PCT/US2002/011239
(87)国際公開番号　WO2002/084459
(87)国際公開日　平成14年10月24日(2002.10.24)
審査請求日　平成15年10月23日(2003.10.23)
(31)優先権主張番号　09/829,761
(32)優先日　平成13年4月10日(2001.4.10)
(33)優先権主張国　米国(US)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)復代理人　100106699
弁理士　渡部　弘道
(74)復代理人　100077584
弁理士　守谷　一雄
(74)代理人　100086243
弁理士　坂口　博

最終頁に続く

(54)【発明の名称】おとりとして無差別システムを使用してネットワーク上の特定のコンピュータ・ウィルスを検出、通知、除去する方法および装置

(57)【特許請求の範囲】

【請求項１】

加害システムとローカル・サーバが接続されたネットワークにおいてコンピュータ・ウィルスの存在を検出する方法であって、

未公開のネットワーク・アドレスを有し、かつユーザのアクセスが禁止されたおとりサーバを前記ネットワークに接続するステップと、

前記おとりサーバが前記加害システムからのアクセス要求を受け取るステップと、

前記おとりサーバが前記アクセス要求を発信した加害システムを識別するステップと、

ウィルス攻撃が進行中であることおよび前記加害システムの識別を前記おとりサーバが前記ローカル・サーバに警告するステップと、

前記おとりサーバが前記ローカル・サーバに前記加害システムを前記ネットワークから切断するよう指令するステップと

を有する方法。

【請求項２】

前記加害システムを切断する前に、前記加害システムにそれがコンピュータ・ウィルスに感染していることを通知するステップを更に有する請求項１に記載の方法。

【請求項３】

加害システムとローカル・サーバが接続されたネットワークにおいてコンピュータ・ウィルスの存在を検出する方法であって、

未公開のネットワーク・アドレスを有し、かつユーザのアクセスが禁止されたおとりサ

ーバを前記ネットワークに接続するステップと、
前記おとりサーバが、前記おとりサーバ内部のファイルを監視するステップと、
前記おとりサーバ内部のファイル中の変更に応答して、前記加害システムからウィルス攻撃が実施されていることを前記ローカル・サーバに通知するステップと
を有する方法。
【請求項４】
前記ファイル中の変更がファイルのバイト・サイズの変更を含む請求項３に記載の方法。
【請求項５】
前記ファイル中の変更がファイルの紛失および削除のいずれかを含む請求項３に記載の方法。
【請求項６】
加害システムとローカル・サーバが接続されたネットワークに接続され、未公開のネットワーク・アドレスを有し、かつユーザのアクセスが禁止されたおとりサーバにおいてコンピュータ・ウィルスの存在を検出するコンピュータ・プログラムであって、前記おとりサーバに、
前記加害システムからのアクセス要求を受け取る機能と、
前記アクセス要求を発信した加害システムを識別する機能と、
ウィルス攻撃が進行中であることおよび前記加害システムの識別情報とを前記ローカル・サーバに警告する機能と、
前記ローカル・サーバに前記加害システムを前記ネットワークから切断するよう指令する機能と
を実現させるコンピュータ・プログラム。
【請求項７】
前記加害システムを切断する前に、前記加害システムにそれがコンピュータ・ウィルスに感染していることを通知する機能を更に実現させる請求項６に記載のコンピュータ・プログラム。
【請求項８】
加害システムとローカル・サーバが接続されたネットワークに接続され、未公開のネットワーク・アドレスを有し、かつユーザのアクセスが禁止されたおとりサーバにおいてコンピュータ・ウィルスの存在を検出するコンピュータ・プログラムであって、前記おとりサーバに、
前記おとりサーバ内部のファイルを監視する機能と、
前記おとりサーバ内部のファイル中の変更に応答して、前記加害システムからウィルス攻撃が実施されていることを前記ローカル・サーバに通知する機能と
を実現させるコンピュータ・プログラム。
【請求項９】
前記ファイル中の変更が、ファイルのバイト・サイズの変更を含む請求項８に記載のコンピュータ・プログラム。
【請求項１０】
前記ファイル中の変更が、ファイルの紛失および削除のいずれかを含む請求項８に記載のコンピュータ・プログラム。
【請求項１１】
加害システムとローカル・サーバが接続されたネットワークに、未公開のネットワーク・アドレスを有し、かつユーザのログオンを禁止するように接続することが可能なシステムであって、
前記加害システムからのアクセス要求を受け取る受信装置と、
前記受信装置が受け取ったアクセス要求を発信した加害システムの識別情報を識別する識別ユニットと、
ウィルス攻撃が進行中であることおよび前記識別情報が識別された加害システムの前記

識別情報を前記ローカル・サーバに警告するウィルス警告ユニットと、
前記識別情報が識別された加害システムを前記ネットワークから切断するように前記ローカル・サーバに指令する切断ユニットと
を有するシステム。
【請求項１２】
前記加害システムを切断する前に、前記加害システムにそれがウィルスに感染していることを通知する通知ユニットを更に有する請求項１１に記載のシステム。
【請求項１３】
加害システムとローカル・サーバが接続されたネットワークに、未公開のネットワーク・アドレスを有し、かつユーザのログオンを禁止するように接続することが可能なシステムであって、
前記おとりサーバ内部のファイル中の変更の有無を監視する監視ユニットと、
前記おとりサーバ内部のファイル中の変更に応答して、ウィルス攻撃が進行中であることを前記ローカル・サーバに通知する通知ユニットと
を有するシステム。
【請求項１４】
前記ファイル中の変更が、ファイルのバイト・サイズの変更を含む請求項１３に記載のシステム。
【請求項１５】
前記ファイル中の変更が、ファイルの紛失および削除のいずれかを含む請求項１３に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無差別システムを用いて、ネットワーク上のコンピュータ・ウィルスのソースを識別する事業サービスを提供する方法および装置に関する。
【背景技術】
【０００２】
コンピュータ・ウィルスの検出は、よく理解されている技術である。Symantec、McAffee、Shiva、Intelなど、ウィルス検出および除去の事業に関わっている大企業がいくつかある。これらの製品の一部、特にSymantecは、社内ネットワーク、すなわちイントラネット上で管理および使用するためのソフトウェアの法人向けバージョンを提供する。この構成では、ウィルス検出クライアント・ソフトウェアを各クライアント・コンピュータにインストールし、ウィルス・チェッカを特定の間隔で走らせてそのクライアント・マシンにウィルスがいるかどうかを調べる。ウィルスが検出されれば、クライアント・プログラムは、ウィルスを検出したことをユーザに知らせ、管理設定に従って、自動的に対処したりあるいはユーザに対処するよう指示を出したりする。
【０００３】
ウィルスが検出されると、ユーザは通常、感染した１つまたは複数のファイルを現行システムで使用しないように、隔離するよう指示される。感染したファイルを隔離すれば、ユーザは、再びシステムの使用を開始することができる。次いで、ユーザは、システム管理者またはＩＴ部門に連絡してウィルスについて警告するよう指示されることもある。
【０００４】
この戦略に伴う問題は、ウィルスが検出される前に、システムが既にかなり損傷されていることがあるということである。ワーム（Syman1）と呼ばれる一部のウィルスは、検出される前に数百、あるいは数千ものファイルを破壊することができる。さらに悪いことには、クライアント・マシンがウィルスを検出したときには、ウィルスはネットワーク上の別のマシンまたはネットワーク・シェアにそれ自体のクローンを作成してしまっていることもある。ネットワーク・シェアから、ウィルスはファイルの抹消および他のクライアント・システムでのそれ自体のクローン作成を開始することができる。ウィルスのソースの

発見、およびネットワーク上のその痕跡の削除には、通常、ネットワーク・サーバをシャットダウンすること、ネットワーク・シェアを削除すること、及び各クライアント・マシンをネットワークから切断してウィルスを駆除することが必要である。

【０００５】

ウィルスが完全に除去されるようにするためには、特定のマシンを適切にウィルス駆除することができるように、ウィルスが発生した場所を知ることが望ましい。しかし、これは、ユーザが抗ウィルス・ソフトウェアをインストールしていないことがあったり、ユーザがダイアルイン接続を行って知らないうちにウィルスを置いてからログオフしてしまっている大型の企業ネットワークでは特に、割り出すのが難しいことがある。ネットワークがウィルス駆除された場合、加害ユーザが再接続すれば再度感染することになる。感染の再発を防ぐために、加害システムを識別することが重要である。

【０００６】

ほとんどの場合、加害ユーザは、気づかずにウィルスを散布している。「ワーム」と呼ばれる種類のウィルスは、ファイルを消去したりファイルの長さをゼロにしたりして、ファイルを実質的に使用できないようにするよう動作する。ワームは一般に、ファイアウォール・ソフトウェアまたはフィルタで認識されず、通常の実行可能な画像またはスクリプト・ファイルのように見せかけてユーザのマシンに届く。ユーザがそのファイルをクリックすると、ファイルは直ちにそれ自体のクローンを作成し、ワームにとって都合のよいホストとなるべきネットワーク上の新しいシステムを探す。都合のよいホストが見つかると、ワームは自分自身をインストールして再度実行し、さらに別の都合のよいホストを探す。こうしたワームは、その厄介な行為を行うのに必要な特権を自分自身に与えるために、都合が良くて無差別なホストを必要とする。ワームは、コンピュータまたはシェアへの書込みアクセス権を有する、ネットワーク上のシステムを探し出し、次いで、その能力を使用して他のシステム上のファイルを削除する。

【０００７】

ほとんどのネットワークでは、システムが、共有媒体としてのあるタイプの共有記憶装置、即ちおそらくは別のコンピュータのハード・ドライブ、にアクセスするのは通常の手法である。この共有媒体はシェアまたはネットワーク・シェアと呼ばれ、ユーザが、一か所に置かれた情報、プログラム、ファイル、および文書を容易に共有するのを可能としている。シェアへのアクセス権を必要とする各システムは、システム管理者またはネットワーク・サーバのポリシーによってそのアクセス権を認可される。シェアへのアクセス権を持たないシステムは、そのシェアに対する読出しや書込みを行うことができない。読出しおよび書込みアクセス権は、シェアへのアクセス権を有する各システムに対して、別々に認可することができる。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

他のシステムによって複製を行うウィルスの場合、ウィルスは、おそらく検出される前に既に複製済みである。この場合、現在のシステムをウィルス駆除しても役に立たない。というのは、ウィルスはもう一度現在のシステム上にすぐにそれ自体を複製してしまうからである。隣接するマシンを実質的にウィルス駆除するためには、各マシンをネットワークから切断してウィルス駆除し、次いで、ネットワークに接続された各クライアントを調べてウィルス駆除した後でネットワーク上に配置し直さなければならない。ワームのソースを見つけて除去しなければならず、そうしないと、再感染の危険性は極端に高い。

【０００９】

これは冗長な手順であり、初心者のユーザまたは管理者には実行が難しいことがある。大型ネットワークを有するほとんどの企業では、潜在的に有害なコンテンツのダウンロードに対するポリシーをもっているが、社員の経験がより浅い小規模な会社では、潜在的に有害なコンテンツをダウンロードしてしまう傾向がより強い。

【００１０】

したがって、管理者側の多大な能力を必要とせずに、ウィルスを検出し、場所を突き止め、除去することを可能にする方法、システム、およびコンピュータ・プログラム記録媒体が望まれる。

【課題を解決するための手段】

【００１１】

本発明は、ウィルスを識別し、場所を突き止め、抹消する方法、コンピュータ・プログラム記録媒体、およびネットワーク・データ処理システムを提供する。一実施形態では、ネットワーク・データ処理システムは、１台のローカル・サーバ、いくつかのクライアント・データ処理システム、および１台のおとりサーバを含む。おとりサーバのアドレスは、クライアントには公開されない。したがって、おとりサーバにアクセスしようとの試みがあれば、アクセスを試みているクライアントにウィルスが存在することを示していることになる。おとりサーバはそれ自体を監視し、おとりサーバにアクセスしようとするクライアントからの試みに応答して、ウィルスの攻撃が進行中であるという指摘を、ネットワーク内部のすべての装置に対して同報通信する。次いで、おとりサーバは、加害クライアントがウィルス駆除されたという指摘を受け取り、かつ加害クライアントをネットワークから切断するまで、加害クライアントによるそれ以上のアクセス要求をすべて無視する。おとりサーバはまた、ローカル・サーバまたはネットワーク管理者あるいはその両方にこの問題および加害クライアントの識別を通知し、加害クライアントのウィルス駆除を開始するのに適した動作を可能にする。

【発明を実施するための最良の形態】

【００１２】

ここで図面を参照すると、図１は、本発明を実施することができるデータ処理システムのネットワークを図式で表したものである。ネットワーク・データ処理システム１００は、本発明を実施することができるコンピュータのネットワークである。ネットワーク・データ処理システム１００は、ネットワーク１０２を含み、このネットワークは、ネットワーク・データ処理システム１００内部で互いに接続されている様々な装置とコンピュータの間の通信リンクを提供するのに使用する媒体である。ネットワーク１０２は、有線通信線や、無線通信リンク、光ファイバ・ケーブルなどの接続を含むことがある。

【００１３】

図示した例では、サーバ１０４が、記憶装置１０６と共に、ネットワーク１０２に接続される。さらに、クライアント１０８、１１０、１１２、ならびにおとりサーバ１５０もネットワーク１０２に接続される。クライアント１０８、１１０、および１１２は、たとえばパーソナル・コンピュータまたはネットワーク・コンピュータであることがある。図示した例では、サーバ１０４は、ブート・ファイル、オペレーティング・システムのイメージ、アプリケーションなどのデータを、クライアント１０８～１１２に提供する。クライアント１０８、１１０、および１１２は、サーバ１０４に対するクライアントである。ネットワーク・データ処理システム１００は、図示していない追加のサーバ、クライアント、他の装置を含むことがある。図示した例では、ネットワーク・データ処理システム１００は、企業や大学が使用するような、イントラネット、ローカル・エリア・ネットワーク（ＬＡＮ）、または、他のタイプの構内ネットワークである。ネットワーク１０２は、ＴＣＰ／ＩＰプロトコル一式などの１組のプロトコルを使用して互いに通信するネットワークおよびゲートウェイの集合体を表す。サーバ１０４はまた、ネットワーク・データ処理システム１００と、たとえばインターネットのこともある外部ネットワーク１８０との間の接続を提供する。

【００１４】

外部ネットワーク１８０は、インターネットとして実現される場合、ＴＣＰ／ＩＰプロトコル一式を使用して互いに通信するネットワークおよびゲートウェイの世界規模の集合体を表す。インターネットの中心部には、データおよびメッセージを中継する多数の商用、行政用、教育用、および他のコンピュータ・システムから構成される主ノードまたはホスト・コンピュータの間にまたがる高速データ通信回線の幹線がある。

【００１５】
「おとりサーバ」１５０と呼ばれる特殊なサーバが、ネットワーク１０２に導入され、ネットワーク・ワーム・ウィルス用の無差別ホストとして作用する。本明細書で使用するウィルスという用語は、ウィルス、ワーム、トロイの木馬、および、データ処理システムまたはネットワークの通常の動作に干渉するように設計された他のあらゆるタイプの有害プログラムを含む。おとりサーバ１５０は、セキュリティ監視ソフトウェアを使用して、おとりサーバ自体へのすべてのネットワーク・トラフィックおよびログオン・トラフィックを監視するように構成される。おとりサーバのマシン名またはＩＰアドレスは告知されず、どのユーザもマシン１５０にログオンすることができない。おとりサーバ１５０に対してネットワーク要求またはログオン要求が行われると、その要求は予期しないものであり、かつネットワーク１０２内部からのものなので、その要求は感染したマシンからおとりサーバ１５０にそれ自体をコピーしようとしているワーム・ウィルスからのものであると、おとりサーバ１５０は結論づけることができる。

【００１６】
ウィルスは、１０８～１１２などのクライアント・コンピュータから起動されると、他の遠隔ファイル・システムまたはネットワーク・シェアへの書込みアクセス権を有する、ネットワーク上の無差別システムの場所を速やかに突き止める。ウィルスは、おとりサーバ１５０にそれ自体をコピーしようと試みるが、おとりサーバ１５０内のパケット監視ソフトウェアが、感染したシステムによるおとりサーバ１５０への書込みの試みを検出し、データを捕捉する。おとりサーバ１５０は、サーバ１０４に直ちに通知し、サーバは、加害システムとの接続を終了し、その後加害システムがネットワーク１０２にログオンまたは接続しようとするどの試みも拒絶する。サーバ１０４は、次いで、業務イベントを使って遠隔管理者に通知し、ｅメールとポケットベルの両方または何れか一方を介してシステム管理者に通知する。

【００１７】
さらなる予防策として、おとりサーバ１５０は、おとりサーバ・ファイルの状態を継続的に監視し、その大きさおよび有効性を継続的に確認する。おとりサーバ１５０のファイルのうちあるファイルの大きさが変わったこと、またはそれがもはや存在しないことをおとりサーバが検出した場合、おとりサーバは、ウィルスが検出されたことをローカル・サーバ１０４にイベントを送ることによって通知し、ローカル・サーバは、どの接続も外し、それ自体と、ネットワーク上の他のコンピュータおよびシェアとに対してウィルス駆除の処理を開始する。何らかの初期損害を受ける前におとりサーバ１５０が常にウィルスのソースを割り出すことができるわけではないが、非常に短時間の間に加害側を捕らえ、損害を最小限に抑える。

【００１８】
したがって、本発明は、能力の高いネットワーク管理者または技術者を必要とせずに、ネットワークに内在するコンピュータ・ウィルスのソースを識別するタスクを実施する、１組のハードウェアおよびソフトウェア構成要素を提供することによって、この問題に対する自動化された解決手段を提供する。この自動化された機能は、おとりサーバ１５０の追加に加え、ネットワーク・サーバ１０２およびクライアント・コンピュータ１０８～１１２にインストールされるソフトウェアの形で提供することができ、またユーザが登録することができる事業サービスとして提供することもできる。

【００１９】
ウィルスがおとりサーバ１５０またはクライアントの抗ウィルス・ソフトウェアによって検出され、かつウィルスがワームである場合、サーバは、ウィルスのソースを見つけ、ウィルスの発生源であるマシンがウィルス駆除されるようにし、その後でそのマシンをネットワーク１０２またはシェアに再接続させなければならない。

【００２０】
本発明を事業サービスとして提供する場合、おとりサーバ１５０は、「ウィルスを検出した」という業務イベントを送ることによって、そしてまた、検出されたウィルスのタイ

プと、ウィルスが検出されたクライアントの名称と、システムをウィルス駆除するために取った処置とに関する情報を含むｅメール・メッセージを送ることによって、直ちに遠隔管理者に通知する。おとりサーバ１５０は、技術者をポケットベルで呼び出すことも、サポート技術者に電話をかけることもできる。通知を受け取ると、管理者イベント中継システムは、同様に他の業務イベントを生成したり、顧客に対するオンサイト・サービス・コールまたは電話呼出しをスケジューリングしたり、技術者をポケットベル呼び出ししたりすることができ、極端な場合には、ローカル・サーバとローカル・エリア・ネットワークの両方または何れか一方をシャットダウンすることもできる。

【００２１】

加害コンピュータを突きとめるために、おとりサーバ１５０は、上で説明したように、ネットワーク上に導入されて「おとり」として振る舞い、ワーム・ウィルスを引き寄せる。ワームとして知られるこの範疇のウィルスは、システム・シェアに対する書込み能力を有する、ウィルスを受け入れるコンピュータを求めて、ネットワークを探し回る。ウィルスは、ネットワーク・サーバの場所を突き止めるために、ＮＥＴＢＩＯＳ同報通信などの様々な技術を使用する。ウィルスは、ＮＥＴＢＩＯＳプロトコルを使用して、他のコンピュータまたはネットワーク・シェアへの書込みアクセス権を有するネットワーク上のサーバの場所を突き止める。次いで、ウィルスは、それ自体を当該サーバにコピーし、それ自体をサービスとしてインストールし、オペレーティング・システムが開始される度またはユーザがログオンする度に当該サービスを起動する。実行されると、ウィルスはローカル・ファイル、遠隔ファイル、およびネットワーク・シェア上のファイルを抹消し始める。直ちに介入しないと、ウィルスは、毎分多数のファイルを抹消または使用不能にすることができる。

【００２２】

おとりサーバ１５０は、ネットワーク１０２上のマシンからのログイン要求およびネットワーク要求を監視するように構成される。おとりサーバ１５０はネットワーク１０２のユーザには知られていないので、おとりサーバ１５０にログオンしようとしたり、またはネットワーク１０２を介してそれにデータを送付しようとする唯一のシステムは、ウィルスそれ自身である。おとりサーバ１５０は、セキュリティ監視が可能なように構成され、すべてのネットワーク要求およびセキュリティ要求が監視される。おとりサーバ１５０は、可能な限りオープンに構成され、実際にはローカル・ディスク・ドライブである孤立した公開ネットワーク・シェアに対して、書込み可能になっている。

【００２３】

このネットワーク・シェア上に、．ＤＯＣ、．ＰＰＴ、．Ｈ、．ＣＰＰ、．Ｃ、．ＡＳＭ、．ＸＬＳなど、通常ワーム・ウィルスの標的となるファイルがインストールされる。一旦ログオン要求がおとりサーバ・マシン１５０に届くと、おとりサーバ１５０は、要求を出しているコンピュータへの接続を直ちに切り、遠隔管理サーバに業務イベントを生成し、システム管理者に優先度の高いｅメール・メッセージを送る。各メッセージは、時刻、日付、加害マシンのＩＰアドレスおよび名称、ならびにウィルスが使おうとしているユーザＩＤおよびパスワードなどの情報を含む。おとりサーバ１５０は、次いで、ウィルス攻撃が行われているというメッセージを、ネットワーク中に同報通信する。

【００２４】

シェアへの書込み要求がおとりサーバ１５０に届いた場合も同じ動作が行われる。やはり、送信元マシンのＩＰアドレス、マシン名、ウィルスのタイプ、および他の情報が集められてローカル・サーバ１０４に中継のために送られる。本発明をうまく働かせるのを可能とする一条件は、ウィルスが、最も無差別なマシンを最初に追跡し、ウィルス自体を早期に露出させるほど「賢い」ことである。

【００２５】

加害マシンのログオン・アカウントは、ネットワーク１０２から一旦削除されると、使用禁止になる。ウィルス・イベントを生成したＩＰアドレスまたはマシン名からのそれ以降の要求は、ネットワークからウィルスが削除され、かつ加害マシンがウィルス駆除され

たと判断されるまで、どれも無視される。こうした判定が行われた時点で、加害マシンはネットワーク１０２に再接続され、ネットワークの通常動作が続行される。

【００２６】

図１は、例示を意図したものであり、本発明のアーキテクチャ上の限定を意図するものではない。

【００２７】

図２を参照すると、本発明による、図１の「おとり」サーバ１５０またはサーバ１０４などのサーバとして実現することができるデータ処理システムのブロック図を示してある。データ処理システム２００は、システム・バス２０６に接続された複数のプロセッサ２０２および２０４を含む、対称型マルチプロセッサ（ＳＭＰ）システムであってもよい。あるいは、単一プロセッサ・システムを採用してもよい。メモリ・コントローラ／キャッシュ２０８もまた、システム・バス２０６に接続され、ローカル・メモリ２０９へのインタフェースを提供する。Ｉ／Ｏバス・ブリッジ２１０は、システム・バス２０６に接続され、Ｉ／Ｏバス２１２へのインタフェースを提供する。メモリ・コントローラ／キャッシュ２０８とＩ／Ｏバス・ブリッジ２１０は、図に示すように統合してもよい。

【００２８】

Ｉ／Ｏバス２１２に接続された、ＰＣＩ（周辺装置相互接続）バス・ブリッジ２１４は、ＰＣＩローカル・バス２１６へのインタフェースを提供する。いくつかのモデムをＰＣＩバス２１６に接続することができる。一般的なＰＣＩバスの実現では、４つのＰＣＩ拡張スロットまたはアドイン・コネクタをサポートする。図１のネットワーク・コンピュータ１０８～１１２への通信リンクは、アドイン・ボードを介してＰＣＩローカル・バス２１６に接続されたモデム２１８およびネットワーク・アダプタ２２０を介して提供することができる。

【００２９】

追加のＰＣＩバス・ブリッジ２２２および２２４は、追加のＰＣＩバス２２６および２２８のためのインタフェースを提供し、この追加のＰＣＩバスから、追加のモデムまたはネットワーク・アダプタをサポートすることができる。このようにして、データ処理システム２００は、複数のネットワーク・コンピュータへの接続を可能にする。メモリ・マップ式のグラフィックス・アダプタ２３０およびハード・ディスク２３２も、図に示すように、直接または間接的にＩ／Ｏバス２１２に接続することができる。

【００３０】

当業者であれば、図２に示したハードウェアが様々な形をとり得ることを理解するであろう。たとえば、図示したハードウェアに加えて、またはその代わりに、光ディスク・ドライブなど他の周辺装置を使用してもよい。図示した例は、本発明に関するアーキテクチャ上の限定の暗示を意味するものではない。

【００３１】

図２に示したデータ処理システムは、たとえば、ＡＩＸ（Advanced Interactive Executive）オペレーティング・システムを実行する、インターナショナル・ビジネス・マシーンズ・コーポレーション（ニューヨーク州アーモンク）の製品であるＩＢＭ　ＲＩＳＣ／Ｓｙｓｔｅｍ　６０００システムであってもよい。

【００３２】

ここで図３を参照すると、本発明に基づく、クライアントとして実現することができるデータ処理システムを示すブロック図を示してある。データ処理システム３００は、たとえば、図１のクライアント１０２～１１０のいずれかといったクライアント・コンピュータの例である。データ処理システム３００は、ＰＣＩ（周辺装置相互接続）ローカル・バス・アーキテクチャを使用する。図示した例ではＰＣＩバスを採用しているが、ＡＧＰ（アクセラレイテッド・グラフィックス・ポート）やＩＳＡ（業界標準アーキテクチャ）など、他のバス・アーキテクチャを使用することもできる。プロセッサ３０２およびメイン・メモリ３０４は、ＰＣＩブリッジ３０８を介してＰＣＩローカル・バス３０６に接続される。ＰＣＩブリッジ３０８はまた、プロセッサ３０２用の統合メモリ・コントローラお

よびキャッシュ・メモリを含むこともある。ＰＣＩローカル・バス３０６への追加接続は、直接的な構成要素相互接続を介して、またはアドイン・ボードを介して行われる。図示した例では、ローカル・エリア・ネットワーク（ＬＡＮ）アダプタ３１０、ＳＣＳＩホスト・バス・アダプタ３１２、および拡張バス・インタフェース３１４が、直接的な構成要素接続によってＰＣＩローカル・バス３０６に接続される。これに対して、オーディオ・アダプタ３１６、グラフィックス・アダプタ３１８、およびオーディオ／ビデオ・アダプタ３１９は、拡張スロットに挿入されたアドイン・ボードによってＰＣＩローカル・バス３０６に接続される。拡張バス・インタフェース３１４は、キーボードおよびマウス・アダプタ３２０、モデム３２２、および追加メモリ３２４用の接続を提供する。ＳＣＳＩ（小型コンピュータ・システム・インタフェース）ホスト・バス・アダプタ３１２は、ハード・ディスク・ドライブ３２６、テープ・ドライブ３２８、およびＣＤ－ＲＯＭドライブ３３０用の接続を提供する。一般的なＰＣＩローカル・バスの実現では、３つまたは４つのＰＣＩ拡張スロットまたはアドイン・コネクタをサポートすることになる。

【００３３】

オペレーティング・システムが、プロセッサ３０２上で稼働し、図３のデータ処理システム３００内部の様々な構成要素の制御を調整かつ提供するのに使用される。当該オペレーティング・システムは、Microsoft Corporationから入手できるＷｉｎｄｏｗｓ（Ｒ）２０００など、市販のオペレーティング・システムでもよい。Ｊａｖａ（Ｒ）などのオブジェクト指向プログラミング・システムが、当該オペレーティング・システムと共に稼働することができ、データ処理システム３００上で実行中のＪａｖａ（Ｒ）プログラムまたはアプリケーションから当該オペレーティング・システムへの呼出しを提供することができる。「Ｊａｖａ（Ｒ）」は、SunMicrosystems, Inc.の商標である。オペレーティング・システム、オブジェクト指向オペレーティング・システム、およびアプリケーションやプログラムに対する命令は、ハード・ディスク・ドライブ３２６などの記憶装置上に配置され、プロセッサ３０２によって実行されるためにメイン・メモリ３０４にロードすることができる。

【００３４】

当業者であれば、図３のハードウェアが実装形態によって変わり得ることを理解するであろう。フラッシュＲＯＭ（または同等の不揮発性メモリ）や光ディスク・ドライブなど、他の内部ハードウェアまたは周辺装置を、図３に示したハードウェアに加えて、またはその代わりに使用することがある。また、本発明の処理は、マルチプロセッサ・データ処理システムにも適用することができる。

【００３５】

別の例として、データ処理システム３００は、それが何らかのタイプのネットワーク通信インタフェースを備えているかどうかに関わらず、何らかのタイプのネットワーク通信インタフェースを利用せずにブート可能なように構成された、独立型のシステムであってもよい。さらに別の例として、データ処理システム３００は、オペレーティング・システム・ファイルとユーザ生成データの両方または何れかを格納する不揮発性メモリを提供するための、ＲＯＭおよびフラッシュＲＯＭの両方または何れかを備えた構成の、携帯情報端末（ＰＤＡ）装置であってもよい。

【００３６】

図３に示した例および上で説明した例は、アーキテクチャ上の限定の暗示を意味するものではない。たとえば、データ処理システム３００は、ＰＤＡの形をとるだけでなく、ノート型コンピュータでも、ハンドヘルド・コンピュータでもよい。データ処理システム３００はまた、キオスクでも、ウェブ機器でもよい。

【００３７】

ここで図４を参照すると、本発明に基づく、コンピュータ・ウィルスを検出し、場所を突き止め、除去するおとりサーバ上で実行するための処理フローおよびプログラム機能を示してある。処理４００は、たとえば、図１のおとりサーバ１５０上で実施することができる。始めに、おとりサーバが４０２で電源オンされ、ウィルス監視を伴う通常動作４０

４を開始する。電源オフ・イベントが起きると（ステップ４０６）、処理は終わる。しかし、おとりサーバが電源オフされるまで、おとりサーバはそれ自体を継続的に監視して、ウィルス・イベントが検出されたかどうかを判断する（ステップ４０８）。

【００３８】

おとりサーバは、たとえば、おとりサーバに対してデータの書込みを試みることなどによっておとりサーバに対して試みられるアクセスを観察することにより、ウィルス・イベントを検出することができる。おとりサーバのアドレスは公開されておらず、ネットワークに対して他の機能を実施しないので、おとりサーバにアクセスしようとの試みはどれも不審であり、ネットワーク上にウィルスが存在することを示している。さらなる予防策として、おとりサーバは、おとりサーバ・ファイルのサイズおよび有効性を継続的に確認して、ファイルの状態を継続的に監視することができる。おとりサーバ・ファイルのうちあるファイルのサイズが変わるか、またはそれがもはや存在しないということをおとりサーバが検出した場合、このことはウィルスの存在を示唆することができる。そこからウィルスがおとりサーバへのアクセスを試みているという加害コンピュータの位置は、おとりサーバへのアクセスを要求しているコンピュータのアドレスに注目することによって識別される。

【００３９】

ウィルス・イベントが検出されない場合、おとりサーバは、通常動作およびウィルス監視を続ける（ステップ４０４）。ウィルス・イベントが検出された場合、おとりサーバは、遠隔管理者にメッセージを送り（ステップ４１０）、ウィルスが検出されたことおよびネットワーク内部のウィルスが発生したコンピュータの識別を、遠隔管理者に知らせる。おとりサーバは、次いで、加害コンピュータ用の接続およびシェアを外し（ステップ４１２）、加害コンピュータに、それ自身からウィルス駆除をするよう命令する（ステップ４１４）。

【００４０】

おとりサーバは、次いで、加害コンピュータからの再接続要求を待つ（ステップ４１６）。再接続要求を受け取らなかった場合（ステップ４１８）、おとりサーバは待機し続ける（ステップ４１６）。しかし、ウィルスが発生した加害コンピュータを識別し、管理者に通知し、加害コンピュータを切断し、かつ再接続要求を待っている期間中でも、おとりサーバは、他のウィルス・イベントに対する自分自身の監視をし続ける。再接続要求を受け取った場合、おとりサーバは加害コンピュータを再接続し（ステップ４２０）、通常動作およびウィルス監視を続ける（ステップ４０４）。

【００４１】

このように、おとりサーバは、比較的素早くウィルスが検出され、削除されることを可能にし、通常は、ネットワークに対する深刻な損害または混乱を防止する。さらに、そこからウィルスが最初にネットワークに入ったというコンピュータの身元を確定することによって、ウィルスがネットワーク内部のさらに多くのコンピュータを感染させる時間を持つ前に、そのコンピュータを切断し、ウィルス駆除をすることができる。

【００４２】

そこからウィルスがネットワークに入ったという加害コンピュータがローカル・サーバである場合、その動作はクライアント・コンピュータと基本的に同じである。おとりサーバは、クライアントにウィルス攻撃メッセージを送り、そのメッセージによってクライアントは切断し、接続を外す。ローカル・サーバは、確実にすべての接続を外すようにし、自分自身をウィルス駆除し、次いで、クライアントが使用可能になったときそれに再接続する。

【００４３】

ここで図５を参照すると、本発明に基づく、ウィルスの存在を検出するための、クライアント上で実施することができる処理フローおよびプログラム機能を示してある。処理５００は、たとえば、図１のクライアント１０８～１１２のいずれにおいても実施することができる。始めに、コンピュータが電源オンされ、ネットワークに接続される（ステップ

５０２）。コンピュータは、次いで、通常動作に入る（ステップ５０４）。電源オフ・イベントが起きると（ステップ５０６）、処理は当然終わる。電源オフ・イベントが起きるまで、コンピュータは通常動作を続け、ウィルスがおとりサーバによって検出されたかどうかを、ネットワークからの通知を待つことによって判断する（ステップ５０８）。コンピュータにウィルスが存在することを示す通知を受け取らなかった場合、コンピュータは通常動作を続ける（ステップ５０４）。

【００４４】

コンピュータにウィルスが存在することを示すウィルス通知を受け取った場合、コンピュータは、たとえば、ディスプレイにメッセージを提示するか、または所有者もしくはユーザをポケットベルで呼び出すことによって、所有者に通知を送ることができる（ステップ５１０）。コンピュータは、次いで、ネットワークから切断され（ステップ５１２）、次いで自分自身をウィルス駆除する（ステップ５１４）。コンピュータは、様々な市販の製品などのウィルス検出および抹消プログラムを自動的に実行することによって、自分自身をウィルス駆除することができる。あるいは、ウィルス駆除処理に、重要なユーザ介入と、おそらくネットワーク管理者など専門家のサービスとが必要となることもある。

【００４５】

コンピュータがウィルス駆除されると、コンピュータは、ネットワークへの再接続要求を送り（ステップ５１６）、その要求が認められるのを待つ。コンピュータは、次いで、要求が認められたかどうかを判断し（ステップ５１８）、認められなかった場合は、待機し続ける。要求が認められた場合、コンピュータは、ネットワークに接続され、通常動作を続ける（ステップ５０４）。

【００４６】

本発明は、完全に機能するデータ処理システムに照らして説明してきたのではあるが、当業者であれば、本発明の処理がコンピュータ可読な命令媒体など様々な形で配布できること、および、本発明が配布の遂行に実際に使用される信号伝達媒体の形式に関わらず等しく適用されることとを、理解するであろうということに留意することは重要である。コンピュータ可読媒体の例としては、フロッピー（Ｒ）・ディスク、ハード・ディスク・ドライブ、ＲＡＭ、ＣＤ－ＲＯＭなど記録可能型媒体や、デジタルおよびアナログ通信リンクなどの伝送型媒体がある。

【００４７】

本発明の説明は、例示および説明の目的で提示したが、網羅的であることを意図するものではなく、あるいは、開示した形の発明に限定されるものではない。多くの変更形態および変形形態が当業者には明らかであろう。本実施形態は、本発明の原理および実際の適用例を最もよく説明するために、また、企図される特定の使用に適する様々な変更を伴った様々な実施形態について、他の当業者が本発明を理解できるようにするために、選択されかつ説明されたものである。

【図面の簡単な説明】

【００４８】

【図１】本発明を実施することができる、データ処理システムのネットワークを図式で表したものである。

【図２】本発明に基づいて、サーバとして実現することができる、データ処理システムのブロック図を表したものである。

【図３】本発明に基づいて、クライアントとして実現することができる、データ処理システムのブロック図を表したものである。

【図４】本発明に基づいて、コンピュータ・ウィルスを検出し、場所を突き止め、除去するための、おとりサーバ上で実行される処理フローおよびプログラム機能を表したものである。

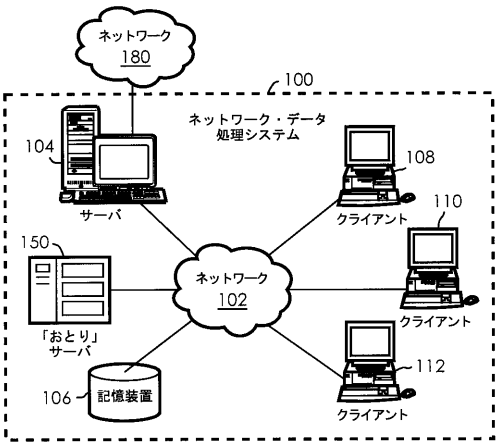
【図５】本発明に基づいて、ウィルスの存在を検出するための、クライアント上で実施することができる処理フローおよびプログラム機能を表したものである。

【符号の説明】

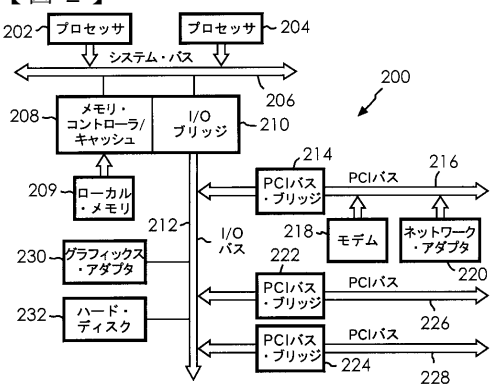
【００４９】
１００　・・・　ネットワーク・データ処理システム
１０２　・・・　ネットワーク
１０４　・・・　サーバ
１０６　・・・　記憶装置
１０８　・・・　クライアント
１１０　・・・　クライアント
１１２　・・・　クライアント
１５０　・・・　「おとり」サーバ
２００　・・・　データ処理システム
２０２　・・・　プロセッサ
２０４　・・・　プロセッサ
２０６　・・・　システム・バス
２０８　・・・　メモリ・コントローラ／キャッシュ
２０９　・・・　ローカル・メモリ
２１０　・・・　Ｉ／Ｏブリッジ
２１２　・・・　Ｉ／Ｏバス
２１４　・・・　ＰＣＩバス・ブリッジ
２１６　・・・　ＰＣＩバス
２１８　・・・　モデム
２２０　・・・　ネットワーク・アダプタ
２２２　・・・　ＰＣＩバス・ブリッジ
２２４　・・・　ＰＣＩバス・ブリッジ
２２６　・・・　ＰＣＩバス
２２８　・・・　ＰＣＩバス
２３０　・・・　グラフィクス・アダプタ
２３２　・・・　ハード・ディスク
３００　・・・　データ処理システム
３０２　・・・　プロセッサ
３０４　・・・　メイン・メモリ
３０６　・・・　バス
３０８　・・・　ホスト／ＰＣＩ　キャッシュ／ブリッジ
３１０　・・・　ＬＡＮアダプタ
３１２　・・・　ＳＣＳＩホスト・バス・アダプタ
３１４　・・・　拡張バス・インターフェース
３１６　・・・　オーディオ・アダプタ
３１８　・・・　グラフィクス・アダプタ
３１９　・・・　オーディオ／ビデオ・アダプタ
３２０　・・・　キーボードおよびマウス・アダプタ
３２２　・・・　モデム
３２４　・・・　メモリ
３２６　・・・　ディスク
３２８　・・・　テープ
３３０　・・・　ＣＤ－ＲＯＭ
４００　・・・　サーバ動作
４０２　・・・　ステップ（処理）
４０４　・・・　ステップ（処理）
４０６　・・・　ステップ（条件分岐）
４０８　・・・　ステップ（条件分岐）
４１０　・・・　ステップ（処理）

４１２　・・・　ステップ（処理）
４１４　・・・　ステップ（処理）
４１６　・・・　ステップ（処理）
４１８　・・・　ステップ（条件分岐）
４２０　・・・　ステップ（処理）
５００　・・・　クライアント動作
５０２　・・・　ステップ（処理）
５０４　・・・　ステップ（処理）
５０６　・・・　ステップ（分岐）
５０８　・・・　ステップ（分岐）
５１０　・・・　ステップ（処理）
５１２　・・・　ステップ（処理）
５１４　・・・　ステップ（処理）
５１６　・・・　ステップ（処理）
５１８　・・・　ステップ（分岐）

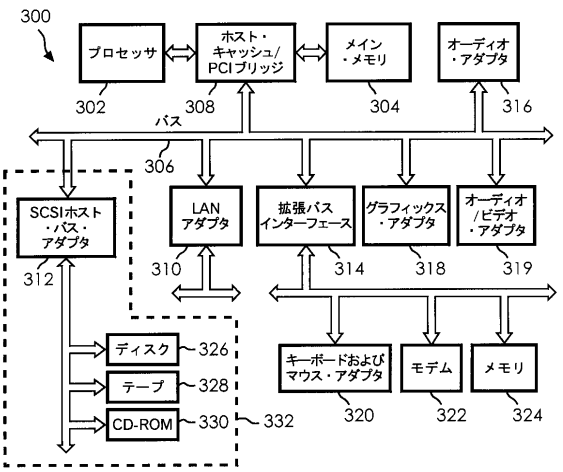
【図１】



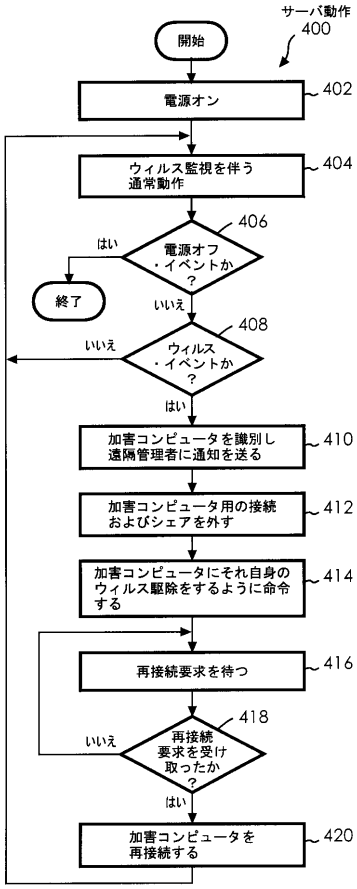
【図２】



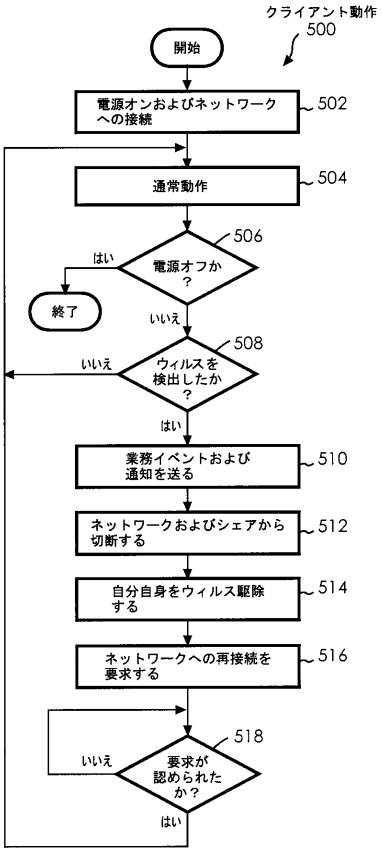
【図３】



【図４】


サーバ動作
400
開始
電源オン
402
ウィルス監視を伴う通常動作
404
406
電源オフ・イベントか？
はい
終了
いいえ
408
ウィルス・イベントか？
いいえ
はい
加害コンピュータを識別し遠隔管理者に通知を送る
410
加害コンピュータ用の接続およびシェアを外す
412
加害コンピュータにそれ自身のウィルス駆除をするように命令する
414
再接続要求を待つ
416
418
再接続要求を受け取ったか？
いいえ
はい
加害コンピュータを再接続する
420

【図５】


クライアント動作
500
開始
電源オンおよびネットワークへの接続
502
通常動作
504
506
電源オフか？
はい
終了
いいえ
508
ウィルスを検出したか？
いいえ
はい
業務イベントおよび通知を送る
510
ネットワークおよびシェアから切断する
512
自分自身をウィルス駆除する
514
ネットワークへの再接続を要求する
516
518
要求が認められたか？
いいえ
はい

フロントページの続き

(74)代理人 100091568
弁理士 市位 嘉宏
(74)代理人 100108501
弁理士 上野 剛史
(72)発明者 シェファラス、トーマス
アメリカ合衆国１０５８９ ニューヨーク州ソマーズ ブライアーウッド・ドライブ ２１４
(72)発明者 マストリアンニ、スティーブン
アメリカ合衆国０６０８５ コネチカット州ユニオンビル グレート・オーク・レーン １５
(72)発明者 モヒンドラ、アジャイ
アメリカ合衆国１０５９８ ニューヨーク州ヨークタウン・ハイツ リン・コート １３４０

審査官 本郷 彰

(56)参考文献 特開平１１－３２７８９７（ＪＰ，Ａ）
特開平０３－２３３６２９（ＪＰ，Ａ）
山口 英, ＵＮＩＸ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｎｏｔｅｓ:１２９, ＵＮＩＸ ＭＡＧＡＺＩＮＥ 第１４巻 第３号, 日本, 株式会社アスキー, １９９９年 ３月 １日, 第１４巻第３号, Ｐ１８, (CS-ND-1999-00768-001)

(58)調査した分野(Int.Cl., ＤＢ名)
G06F 21/22
G06F 13/00
G06F 12/00
G06F 21/20