(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4828193号
(P4828193)
(45)発行日　平成23年11月30日(2011.11.30)　(24)登録日　平成23年9月22日(2011.9.22)

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

請求項の数 8 (全 12 頁)

(21)出願番号　特願2005-284423(P2005-284423)
(22)出願日　平成17年9月29日(2005.9.29)
(65)公開番号　特開2006-127498(P2006-127498A)
(43)公開日　平成18年5月18日(2006.5.18)
審査請求日　平成20年9月29日(2008.9.29)
(31)優先権主張番号　10/976,567
(32)優先日　平成16年10月29日(2004.10.29)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ミハイ　コスティア
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】文書へのアンチウイルスマニフェストのスタンピング

(57)【特許請求の範囲】
【請求項１】
アンチウイルスプログラムによってファイルをスキャンする方法であって、
複数のファイルの少なくとも１つを識別すること、
前記識別されたファイルの付加情報と、前記識別されたファイルに関連付けられたアンチウイルス状態情報とを取得して、前記識別されたファイルが前記アンチウイルスプログラムによるスキャンが必要であるか判定すること、
前記識別されたファイルがスタンプを含むか否か判定することであって、前記スタンプは、コンピュータ関連ウイルスの感染の影響を受けやすいデータセクションのアドレス位置をファイル内で識別すること、
前記識別されたファイルが前記スタンプを含む場合、前記スタンプを解析して、前記識別されたファイルの中でウイルスの影響を受けやすいと識別されたデータセクションを判定すること、および前記データセクションのみを前記アンチウイルスプログラムによりスキャンすること、
前記識別されたファイルが前記スタンプを含まない場合、前記識別されたファイルの全てのセクションを前記アンチウイルスプログラムによりスキャンすること、および
前記識別されたファイルに関連付けられた前記アンチウイルス状態情報を更新すること
を備えたことを特徴とする方法。
【請求項２】
前記スタンプは、前記ファイルが作成される時に作成され、前記ファイルと関連付けら

れることを特徴とする請求項１に記載の方法。
【請求項３】
前記スタンプは、前記ファイルが作成された後に作成され、前記ファイルと関連付けられることを特徴とする請求項１に記載の方法。
【請求項４】
いずれかのウイルスが発見されると、前記識別されたデータセクションにあるウイルスを駆除することをさらに備えたことを特徴とする請求項１に記載の方法。
【請求項５】
前記スタンプ内で識別されたデータセクションの位置は、実行可能なコンピュータコードと関連付けられたファイル内のアドレス位置であることを特徴とする請求項１に記載の方法。
【請求項６】
前記スタンプ内で識別されたデータセクションの位置は、マクロと関連付けられたファイル内のアドレス位置であることを特徴とする請求項１に記載の方法。
【請求項７】
前記スタンプ内で識別されたデータセクションの位置は、実行可能なコンピュータコードおよびマクロと関連付けられたファイル内のアドレス位置であることを特徴とする請求項１に記載の方法。
【請求項８】
プロセッサをプログラミングするのに使用するシステムであって、
前記プロセッサに請求項１ないし７に記載の方法を実行させる少なくとも１つの埋め込まれたコンピュータプログラムを含む少なくとも１つのコンピュータ読取り可能ストレージデバイス
を備えたことを特徴とするシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般に、コンピュータウイルスの検出に関し、より詳細には、ウイルススキャンに関する。
【背景技術】
【０００２】
アンチウイルス（ＡＶ）プログラムは、ファイルシステムにあるファイルがコンピュータウイルスに感染するのを防止するよう設計されている。一般的に、ＡＶプログラムは、ユーザまたはユーザのアプリケーションとコンピュータのファイルシステムとの間に位置し、コンピュータウイルスに感染したファイルがそのファイルシステムに書込まれないように保証する。ウイルスに感染したファイルがファイルシステムにすでにある場合には、その感染ファイルを実行することや、他のコンピュータにコピーすることがないように保証するのに、ＡＶプログラムが役立つ。
【０００３】
ＡＶプログラムは、各ファイルを、「ウイルスシグネチャファイル」に格納された「ウイルスシグネチャ」のリストと比較することによって、既知のウイルスに関してコンピュータファイルをスキャンする。このスキャンは、アプリケーションを使用するなど、大容量ストレージデバイス上でファイルがアクセスされる時、ユーザの要求に応じて、または予定された通りに、行われる。そのためウイルススキャンは、特にアクセス／リアルタイムのスキャンの場合に、リソース集約的（ＣＰＵおよびディスクＩ／Ｏ）で、かつ処理時間の消費が大きいタスクである。ファイルをスキャンし、場合によってはウイルスを除去するまで、ユーザのファイルオープン要求が遅延されなければならないこともよくある。このようにリソースを消費するため、コンピュータ全体の性能の低下およびユーザへの応答時間を遅らせることにつながりかねない。
【０００４】

各種のＡＶスキャン技術が、今日の当業界で現在使用されている。このような技術は、一組のパラメータ「ＡＶ状態」を、最後のウイルススキャンが行われた時点で各ファイルに保存する概念を含み、あるファイルをスキャンし、感染が見つからなければ、そのファイルが一部変更されない限り再度のスキャンは必要とされない。ＡＶ状態のために選択されたパラメータは、ファイルへのウイルスの侵入の可能性を示すこともでき、ファイルの長さ、チェックサム／フラグ、またはファイルの書込み操作が最後に行われた日付等である。

【０００５】

一般的なＡＶスキャン技術の１つは、ＡＶプログラムの最新の実行中にスキャンしたファイルのＡＶ状態を含むメモリ内のキャッシュまたはディスク上のキャッシュを作成することである。このキャッシュは、あるファイルがアクセスされる時はいつでも、または予定されたスキャンがなされるべき時にはいつもチェックされる。ファイルのＡＶ状態がキャッシュ内にある場合は、スキャン情報キャッシュ内のファイルについてのＡＶ状態パラメータが、ファイルの現在のパラメータに対してチェックされる。両方のパラメータがマッチした場合は、ウイルススキャンをする必要はない。パラメータがマッチしなかった場合か、そのファイルについてのＡＶ状態がキャッシュされていない場合は、ファイルをスキャンし、キャッシュ情報を更新する。

【０００６】

別の手法は、外部のデータベース内にＡＶ状態（大抵はちょうどチェックサム／フラグである）を格納し、ＡＶ状態を、ファイルがアクセスされたときに、ＡＶ状態パラメータの現在値と比較する。この技術は、通常、ＡＶ状態情報が、無許可の変更に対して完全に安全である場合にのみ有効である。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

上述のＡＶスキャン技術は、一般的に、スキャンが必要なファイルの基本的なフォーマットを理解するのに、ＡＶプログラムの設計者が必要である。具体的には、ＡＶプログラムの設計者は、各種のソフトウェアアプリケーションによって生成されたファイルを評価し、それによって設計されたＡＶプログラムは、各種アプリケーションによって生成された「ファイルフォーマット」を成功裡にスキャンすることが可能になる。ソフトウェアアプリケーションの数が増えること、そのため異なるファイルフォーマットの数も増えることに伴い、ＡＶプログラムの設計者にとって、ソフトウェアアプリケーションによって生成および使用されるファイルフォーマットの数が増え続けることに追いついていくことは、極めて困難である。

【課題を解決するための手段】

【０００８】

本発明の例示的な実施形態は、一般的にコンピュータ関連ファイルのスキャンの効率を良くする技術を提供する。あるファイルを作成した時点で、そのファイルを作成するアプリケーションは、スタンプを生成し、作成したファイルと関連付ける。代わりに、コンピュータ関連ウイルスの影響を受けかねないアドレス領域を識別するよう設計されたアプリケーションによって、スタンプを生成し、そのスタンプを既存ファイルと関連付けてもよい。スタンプは、コンピュータに関するウイルス、および／またはマルウェアによって侵入されかねないデータのアドレス位置を含む。このスタンプを使用することによって、アンチウイルスプログラムが、ウイルス感染に関してスキャンされるべきファイルの特定部を迅速に識別することができる。スキャン処理中、ファイル内の他のデータは、無視される。

【０００９】

本発明にかかる例示的な方法は、ファイルと関連付けられたスタンプに従ってコンピュータ関連ウイルスについてのファイルをスキャンすることを含み、スタンプは、コンピュータ関連ウイルスの感染の影響を受けやすいファイルのアドレス位置を識別する。

【００１０】
本発明にかかる別の例示的な方法は、コンピュータファイルを作成し、コンピュータファイルは関連付けられたデータを有すること、コンピュータファイルに関連付けられたデータを評価して、少なくとも１つのコンピュータ関連ウイルスによって破損されかねないデータか否かを判定すること、およびコンピュータ関連ウイルスによって破損されやすいと判定されたデータのアドレス位置の少なくとも１つを含むスタンプを生成することを含む。
【００１１】
本発明によって形成された別の例示的な実施形態は、プロセッサのプログラミングで使用する製品である。この製品は、少なくとも１つのコンピュータ読取り可能ストレージデバイスを含む。コンピュータ読取り可能ストレージデバイスは、埋め込まれた少なくとも１つのコンピュータプログラムを含み、コンピュータプログラムは、プロセッサに本発明による方法を実践させ、その方法は、上述した例示的な方法を含む。
【発明を実施するための最良の形態】
【００１２】
本発明の上記の態様および付随する利点の多くは、添付図面と併せて、下記の詳細な説明を参照することによってその態様および利点への理解が深まるのに伴い、容易に理解されよう。
【００１３】
本発明の例示的な実施形態の以下の詳細な説明において、本発明の例示的な実施形態を図によって示した添付図面を参照する。本発明の実施形態は、当業者が本発明を実施できるように十分詳細に説明される。また、他の実施形態を利用してもよいこと、ならびに本発明の範囲から逸脱せずに、論理的、機械的、電気的な変更および他の変更を加えてもよいことを理解されたい。このように以下の説明は、制限を加えるものではなく、本発明の範囲は、添付の請求項によってのみ定義される。
【００１４】
（序論）
下記の説明は、いくつかの異なるセクションに分けられている。まず始めに、動作環境を開示し、本発明の例示的な実施形態を実装することができる各種ハードウェアの例を提供する。次に、システムレベルの概観を開示し、アンチウイルスプログラムがファイルと持つ相互作用についての考察を含む。各ファイルは、本発明の例示的な実施形態によるスタンプを有し、コンピュータのファイルシステムに格納される。最後に、本発明の実施例にかかる各種方法を開示する。図は、詳細にわたって参照され、本発明の実施形態を理解するのを助ける。
【００１５】
（動作環境）
図１および２の以下の説明は、本発明を実装するのに適したコンピュータハードウェアおよび他のコンポーネントの概観を提供することを目的としたものであり、本発明の実施が可能な適用環境を制限するためのものではない。ハンドヘルド装置、マルチプロセッサシステム、マイクロプロセッサベースかプログラム可能な家庭用電化製品、ネットワークパーソナルコンピュータ（ＰＣ）、ミニコンピュータ、メインフレームコンピュータなどを含む他のコンピュータシステムの構成で本発明を実施することもできることが、当業者には即座に理解できる。また本発明は、通信ネットワークを介してリンクされたリモート処理装置によってタスクが行われる分散コンピューティング環境で実施されてもよい。
【００１６】
図１は、ローカルエリアネットワーク（ＬＡＮ）またはインターネット等のネットワーク１６を介して連結された、いくつかのコンピュータシステム１０を示す。「インターネット」という用語は、本明細書中で、数あるネットワークのうちのある１つのネットワークを呼ぶのに使用される。この１つのネットワークは、ＴＣＰ／ＩＰ（Transmission Control Protocol/Internet Protocol）などのある種のプロトコルを使用し、また場合によ

っては、ワールドワイドウェブ（ＷＷＷ）を構成するＨＴＴＰ（Hypertext Transfer Protocol）文書またはＨＴＭＬ（Hypertext Markup Language）文書等の他のプロトコルを使用する。インターネットの物理的な接続、インターネットのプロトコル、および通信手順は、当業者には公知のものである。

【００１７】

ネットワーク１６へのアクセスは、ＩＳＰ１８およびＩＳＰ２０等のインターネットサービスプロバイダ（ＩＳＰ）によって典型的に提供される。クライアントコンピュータ装置２４、２８、３６、３８等のクライアントシステム上のユーザは、ＩＳＰ１８およびＩＳＰ２０等のインターネットサービスプロバイダを経由してインターネットへのアクセスを得る。インターネットへのアクセスによって、クライアントコンピュータ装置のユーザは、情報を交換すること、電子メールを送受信すること、およびＨＴＭＬフォーマットで用意された文書等を見ることが可能になる。大抵、これらの文書は、インターネット「上」にあると考えられるウェブサーバ２２等のウェブサーバによって提供される。大抵、これらのウェブサーバは、ＩＳＰ１８等のＩＳＰによって提供される。

【００１８】

ウェブサーバ２２は、典型的に、少なくとも１つのコンピュータシステムであり、そのコンピュータシステムは、サーバコンピュータシステムとして動作し、ＷＷＷのプロトコルで動作するように構成される。任意で、ウェブサーバ２２は、クライアント装置のためにインターネットへのアクセスを提供するＩＳＰの一部であってもよい。ウェブサーバ２２は、サーバコンピュータ１４に結合されて図示され、サーバコンピュータ１４はウェブコンテンツ１２に結合されている。ウェブコンテンツ１２は、メディアのデータベースであると考えることもできる。２つのコンピュータシステム２２、１４が図１に示されているが、ウェブサーバ２２およびサーバコンピュータ１４は、１つのコンピュータシステムであってもよく、そのシステムは、ウェブサーバとしての機能性およびサーバとしての機能性を提供する異なるソフトウェアコンポーネントを有することが理解されよう。

【００１９】

クライアントコンピュータ装置２４、２８、３６、および３８は、適切なウェブ閲覧ソフトウェアを用いて、それぞれがウェブサーバ２２によって提供されたＨＴＭＬのページを見ることもできる。ＩＳＰ１８は、通信装置２６経由で、クライアント装置２４にインターネット接続を提供する。通信装置２６は、クライアント装置２４の一部と考えることもできる。クライアント装置２４は、ＰＣ、またはＰＣに類似した他のコンピュータシステムであってよい。同様に、ＩＳＰ２０は、クライアント装置２８、３６、および３８にインターネット接続を提供する。クライアント装置２８は、通信装置３０経由でＩＳＰ２０に結合され、一方クライアント装置３６および３８は、ＬＡＮの一部である。クライアント装置３６および３８は、ネットワークインタフェース４０および４２経由でＬＡＮバス３４に結合され、このネットワークインタフェースは、イーザネットネットワークのインタフェースまたは他のネットワークインタフェースであってもよい。ＬＡＮバス３４は、ゲートウェイコンピュータシステム３２にも結合され、ゲートウェイコンピュータシステム３２は、ファイヤーウォールおよび他のインターネット関連のサービスをＬＡＮのために提供する。ゲートウェイコンピュータシステム３２は、ＩＳＰ２０に結合されて、クライアント装置３６および３８にインターネット接続を提供する。ゲートウェイコンピュータシステム３２は、従来のサーバコンピュータシステムであってもよい。また、ウェブサーバ２２は、従来のサーバコンピュータシステムであってもよい。

【００２０】

代わりに、公知のように、ネットワークインタフェース４６経由でＬＡＮバス３４にサーバ装置４４が直接結合されて、ゲートウェイシステム３２経由でインターネットへの接続を必要とせずに、クライアント装置３６および３８にファイル４８および他のサービスを提供することもできる。

【００２１】

図２は、クライアント装置、サーバ装置、またはウェブサーバとして使用することもで

きるコンピュータシステム６０の例示的な例を示す。また、コンピュータシステム６０は、ＩＳＰ１８および１０７等のインターネットサービスプロバイダの機能の多くを働かせるために使用されてもよいことも理解されよう。コンピュータシステム６０は、通信装置またはネットワークインタフェース６２経由で外部システムにインタフェースする。通信装置またはネットワークインタフェース６２は、コンピュータシステム６０の不可欠な部分であってもよいことが理解される。インタフェース６２は、アナログモデム、ＩＳＤＮモデム、ケーブルモデム、トークンリングインタフェース、またはあるコンピュータシステムを他のコンピュータシステムに結合するための他のインタフェースであってもよい。

【００２２】

コンピュータシステム６０は、処理ユニット６４を含む。処理ユニット６４は、Ｉｎｔｅｌ（登録商標）Ｐｅｎｔｉｕｍ（登録商標）マイクロプロセッサまたはモトローラ社のＰｏｗｅｒＰＣ（登録商標）マイクロプロセッサ等の従来のマイクロプロセッサであってもよい。プロセッサ６４に、バス６６を介してメモリ６８が結合される。メモリ６８は、ＤＲＡＭ（Dynamic Random Access Memory）であってもよく、またＳＲＡＭ（Static RAM）を含んでもよい。バス６６は、メモリ６８にプロセッサ６４を結合させる。また、不揮発性ストレージ７４、ディスプレイコントローラ７０および入力／出力（Ｉ／Ｏ）コントローラ７６にもプロセッサ６４を結合させる。

【００２３】

ディスプレイコントローラ７０は、ディスプレイ装置７２上のディスプレイを従来の方法で制御する。ディスプレイ装置７２のディスプレイは、ブラウン管（ＣＲＴ）または液晶ディスプレイ（ＬＣＤ）であってもよい。入力／出力装置７８は、キーボード、ディスクドライブ、プリンタ、スキャナ、およびマウスまたは他のポインティングデバイスを含む他の入力および／または出力装置を含むこともできる。ディスプレイコントローラ７０およびＩ／Ｏコントローラ７６は、公知の従来技術によって実装されてもよい。

【００２４】

デジタル画像入力装置８０としては、コンピュータシステム６０にデジタルカメラからの画像の入力を可能にするように、Ｉ／Ｏコントローラ７６に結合されたデジタルカメラとすることもできる。不揮発性ストレージ７４は、大抵、磁気ハードディスク、光ディスク、または大容量のデータ用ストレージの他の形態である。このデータのいくらかは、コンピュータシステム６０でのソフトウェアの実行中に、直接的なメモリアクセス処理によって、メモリ６８に書込まれる。「コンピュータ読取り可能媒体」という用語には、処理ユニット６４によってアクセス可能な、どの種類のストレージでも含まれることが、当業者には即座に認識されよう。

【００２５】

コンピュータシステム６０は、異なるアーキテクチャを有することのできる多くのコンピュータシステムの一例に過ぎないことが理解される。例えば、ＰＣは、大抵複数のバスを有し、その１つは、周辺バスであると考えられる。典型的なコンピュータシステムは、通常、プロセッサ、メモリ、およびメモリをプロセッサに結合するバスを含む。

【００２６】

コンピュータシステム６０は、ディスクオペレーティングシステム等のファイル管理システムを含むオペレーティングシステムソフトウェアによって制御され、そのディスクオペレーティングシステムは、オペレーティングシステムソフトウェアの一部であることが当業者には明らかである。関連するファイル管理システムソフトウェアを備えたオペレーティングシステムソフトウェアの一例は、Ｗｉｎｄｏｗｓ（登録商標）オペレーティングシステムであり、これはワークステーションおよびサーババージョンを含む。このようなオペレーティングシステムのファイル管理システムは、典型的に、不揮発性ストレージ７４に格納され、オペレーティングシステムに必要な各種作動をプロセッサ６４に実行させ、メモリへのデータの入力および出力とデータの格納を行う。これは、不揮発性ストレージ７４にファイルを格納することを含む。

【００２７】

（システムレベルの概観）
図３および図４を参照して、本発明の例示的な実施形態の動作のシステムレベルの概観を説明する。図３に示したように、図１のサーバコンピュータ１４などのコンピュータ、またはクライアント装置２４、２８、３６および３８などのクライアント装置に、アンチウイルスプログラム３０２を組み込むこともできる。図２と併せて前述したようなオペレーティングシステムの一部として含まれたファイルシステムが、図２に示した不揮発性ストレージ７４等の不揮発性ストレージに格納されたファイルへのアクセスを制御する。

【００２８】
図３は、アンチウイルスプログラム３０２の使用を含むファイルシステム３００を示す。ファイルシステム３００は、ファイル３０１の各々のために、エントリデータ構造ディレクトリ３０６を維持する。エントリデータ構造ディレクトリ３０６は、ファイル３０１の各々についてファイルタイプ、ファイル識別子、作成日等の情報を保持する。この情報は、エントリデータ構造ディレクトリ３０６の様々なフィールド３０８に格納されている。図３では、１つのファイル３０１のみを示すが、当業者は、ファイルシステム３００に複数のファイルを組み込んでもよいことを理解されよう。

【００２９】
ファイル３０１が、ファイルシステム３００によって、作成されるか、使用またはアクセスされた場合に、アンチウイルスプログラム３０２は、既知のウイルスに関してファイル３０１をスキャンする（符号１）。アンチウイルスプログラム３０２は、１つまたは複数のデータベースエントリ３０４のファイル３０１に関連したＡＶ状態情報を格納する（符号２）。このデータベースエントリ３０４は、アンチウイルスプログラム３０２と関連付けられる。当業者には理解されるように、このＡＶ状態情報３０４は、暗号化した形態にして、ウイルスなどによる悪意ある変更から保護することもできる。アンチウイルスプログラム３０２は、状態情報３０４の書込みと同時に、エントリデータ構造ディレクトリ３０６とインタフェースして（符号３）、ファイル３０１に関連した情報を得る。この情報は、ファイルタイプ、ファイル識別子、および作成日などを含んでもよい。またこの情報は、ファイル３０１がウイルスに関してスキャンされるべき時および頻度についてアンチウイルスプログラム３０２が判定するのを助けるために、状態情報３０４とともに含まれる。例えば、アンチウイルスプログラム３０２がファイル３０１を最後にスキャンしてから、ファイル３０１の作成日が変えられている場合、アンチウイルスプログラム３０２は、データ構造ディレクトリ３０６に格納されたファイル作成日と状態情報３１５とを比較することによって、この判定をなす。比較によって相違が示された場合は、アンチウイルスプログラム３０２は、この判定がなされた特定の時点でファイル３０１をスキャンする。当業者であれば気付くように、アンチウイルスプログラム３０２は、ファイル作成日以外の他の理由のために、ファイル３０１をスキャンする判定をなすこともできる。例えば、作成データも格納されている場合に、ファイル３０１を直接スキャンすることで、アンチウイルスプログラム３０２がウイルスに関してファイル３０１のスキャンを進めるべきかどうかを判定してもよい。

【００３０】
図４は、図３に示したファイル３０１の構造を示す。図示したように、ファイル３０１は、スタンプ（後述する）および追加情報４０２～４１８を含む。追加情報によってファイルシステム３００は、オペレーティングシステムの要件および／または他のアプリケーションの要件による必要に応じて、ファイル３０１を使用し、かつアクセスすることができる。ファイル３０１のファイル名セクション４０２は、ファイル３０１のファイル名を保持するように設計されたものである。フィールド４０４は、ファイル３０１の作成日を保持するよう指定された領域である。追加フィールド４０６～４１８は、ファイル３０１の実際のデータコンテンツを構成する。

【００３１】
フィールドセクション４０６および４１２は、マルウェアまたは他のコンピュータウイルスによって感染されかねない実行可能なコードを含む。フィールドセクション４１０、

４１６、および４１８は、マルウェアまたは他のコンピュータ関連ウイルスによって、やはり感染されかねないマクロエントリを含む。フィールドセクション４０８および４１４は、プレーンテキストを含み、このテキストは、一般的に、マルウェアおよびコンピュータ関連ウイルスの影響を受けない。図４に図示したファイル３０１の構造は、例示のためだけに示されたものである。具体的には、当業者であれば気付くように、ファイルの構造は大きく変わってもよい。具体的には、図示のテキストまたはマクロセクションを含まないファイルがあってもよい。この代わりに、いくつかのファイルは、ファイル識別子（４０２および４０４）で構成されてもよく、残りのファイルを実行可能なコードだけで作ってもよい。他の複数のファイルタイプおよび構造が、当業者によって同様に理解される。

【００３２】

図５は、図４に示したスタンプ４００のボディを示す。スタンプ４００は、実行可能なコードのセクション５００および実行可能なマクロセクション５０２を含む。実行可能なコードのセクション５００は、ファイル３０１に含まれた実行可能なコードのアドレス位置を含む。この場合、実行可能なコードのセクション５００内で、アドレス４０６およびアドレス４１２が識別される。同様に、実行可能なマクロセクション５０２は、ファイル３０１に含まれたマクロアドレス位置を含む。この場合、実行可能なマクロセクション５０２内で、アドレス４１０および４１６が識別される。

【００３３】

前述したように、従来のアンチウイルスプログラムは、一般的に、特定のファイルを効率よくスキャンする前に、そのファイルタイプの構造を理解する必要がある。具体的には、アンチウイルスプログラムは、マルウェアまたは他のコンピュータ関連ウイルスが殺到する実行可能なコード、マクロ、および他のファイルのアドレス位置を理解しなくてはならない。一般的に、アンチウイルスの開発者は、ファイルのファイルタイプ構造をリバースエンジニアリングして、マルウェアまたは他のコンピュータ関連ウイルスがある可能性のある特定の位置を見つけることが必要である。特定のファイルの構造が理解されない場合は、アンチウイルスプログラムは、マルウェアおよび他のコンピュータ関連ウイルスによって影響を受けていないアドレス領域を含むファイルの全部分をスキャンしなくてはならないこともある。明らかにこれは、コンピュータ関連ウイルスに関し所与の任意のファイルをスキャンするのに有効な方法ではない。

【００３４】

本発明の例示的な実施形態にかかるスタンプ４００は、前述の問題を是正する。つまり、アンチウイルスプログラム３０２などのアンチウイルスプログラムは、ファイル３０１などのファイルがコンピュータ関連ウイルスの存在に対してスキャンする前に、スタンプ４００のコンテンツを簡単に再検討しなければならない。

【００３５】

（本発明の典型的な実施形態の方法）

前のセクションでは、本発明の例示的な実施形態の動作のシステムレベルの概観を説明した。このセクションでは、本発明の例示的な実施形態の具体的な方法を、一連のフローチャートを参照してコンピュータソフトウェアの観点から説明する。この方法は、コンピュータで実行可能な命令で作られたコンピュータプログラムを含むコンピュータによって実践することができる。フローチャートを参照し、例示的な実施形態の方法を説明することで、一当業者がそのような命令を含むプログラムを開発して、適切に構成されたコンピュータ（コンピュータ読取り可能媒体からの命令を実行するプロセッサまたはコンピュータ）上で、その方法を実践することができる。公認の標準規格に適合したプログラム言語で書込まれた場合は、そのような命令は、各種のハードウェアプラットフォーム上で実行することができ、また、各種のオペレーティングシステムへのインタフェースのために実行することができる。

【００３６】

本発明の例示的な実施形態は、何か特定のプログラム言語を参照して説明するものではない。各種のプログラム言語を使用して、ここに説明したような本発明の教示を実装して

よいことを理解されたい。さらに、当技術分野では、何らかの作用をすることまたはその結果を生じることとして、ソフトウェアについて１つまたは別の形態（例えばプログラム、処理、手順、アプリケーションなど）で述べることは普通である。このような表現は、コンピュータによるソフトウェアの実行が、コンピュータのプロセッサにある作動を行わせること、または何らかの結果を生じさせることを手短に述べたものに過ぎない。

【００３７】

図６は、本発明の例示的な実施形態にかかるスタンプ４００を含むファイルを作成するためのフローチャートを示す。図６のフローチャートによって示したプロセスは、図１～５と併せて説明したいずれの実施形態でも動作できることは明白である。あるファイルが作成および／または変更されなくてはならないという確認応答がなされた場合に（Ｓ６００）、ファイルシステムまたは他のソフトウェアアプリケーションが、予想ファイルのためにデータ構造をスキャンする（Ｓ６０２）。データ構造のスキャンは、コンピュータ関連ウイルスによって侵入される可能性のあるデータ構造の領域を判定するよう設計される（Ｓ６０４）。具体的には、前のセクションで述べたように、この領域は、一般的に、実行可能なコードおよび／または実行可能なマクロを含む。しかし、ファイルに含まれた他のデータもコンピュータ関連ウイルスの影響を受ける可能性がある。予想ファイルに関するデータ構造の特定の攻撃を受けやすい領域を識別すると、この代表的なデータ構造に関連付けたスタンプを含むファイルを作成する（Ｓ６０６）。このスタンプは、コンピュータ関連ウイルスの攻撃を受けやすいデータ構造部分を識別し、また、ファイルのスキャンが必要と判断された場合に、どこがアンチウイルスプログラムによって分析されるべきなのかを識別する。

【００３８】

図７は、本発明の例示的な実施形態にかかるスタンプ４００を含むファイルをスキャンするのに使用されるプロセスのフローチャートを示す。アンチウイルスプログラムが実行された（Ｓ７００）後、ユーザ対話または予定されたイベントによって、複数のファイルの少なくとも１つが、ＡＶプログラムによるスキャンが必要であると識別される（Ｓ７０２）。ファイルが識別されると、ＡＶプログラムは、簡単にそのファイルを分析する（Ｓ７０４）。分析されたファイルがスタンプを含む場合（Ｓ７０６）、そのスタンプは、解析されてウイルスの影響を受けやすいと識別されたファイルのセクションを判定する（Ｓ７０８）。前述したように、ウイルスの影響を受けやすいファイルのセクションは、一般的に、実行可能なコードまたはマクロを含む。ウイルスの影響を受けやすいと識別されたこのセクションのみが、ＡＶプログラムによってスキャンされる（Ｓ７１０）。識別されたファイルがスタンプを含まない場合、ＡＶプログラムは、従来の方式でそのファイルをスキャンする（Ｓ７１２）。従来の方式にかかるスキャン方法は、識別されたファイル内に含まれた全コンテンツをスキャンしなくてはならないことを含む可能性がある。識別されたファイルをどちらの方式でスキャンするかに関係なく、スキャンが完了すると、ＡＶプログラムの前回のスキャン以来変更されなかったファイルに対する不必要なスキャンを実質的に防止するために、スキャンしたファイルに関するＡＶ状態情報をファイルシステム内で更新する（Ｓ７１４）。

【００３９】

本発明の例示的な実施形態を図示および説明したが、本発明の精神および範囲から逸脱せずに、この実施形態に各種変更を加えることができることが理解されよう。

【図面の簡単な説明】

【００４０】

【図１】ローカルエリアネットワーク（ＬＡＮ）またはインターネット等のネットワーク経由で連結された数個のコンピュータシステムを示す図である。

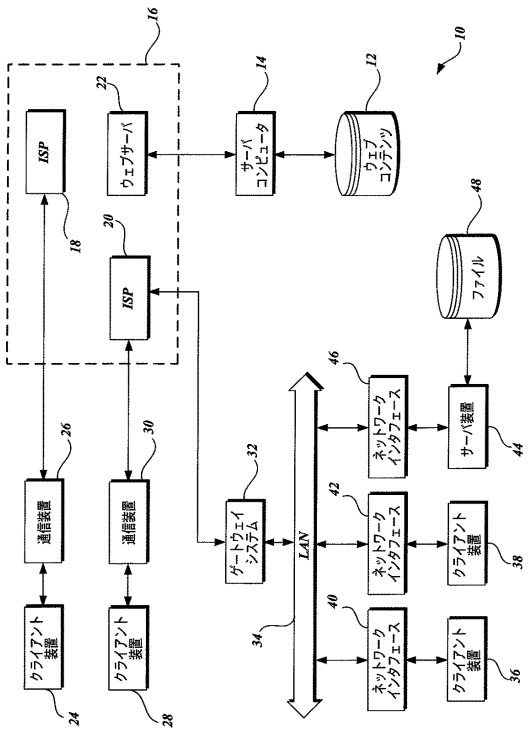
【図２】クライアント装置、サーバ装置、またはウェブサーバとして使用してもよいコンピュータシステムの実施例を示す図である。

【図３】本発明の例示的な実施形態の動作のシステムレベルの概観を示す図である。

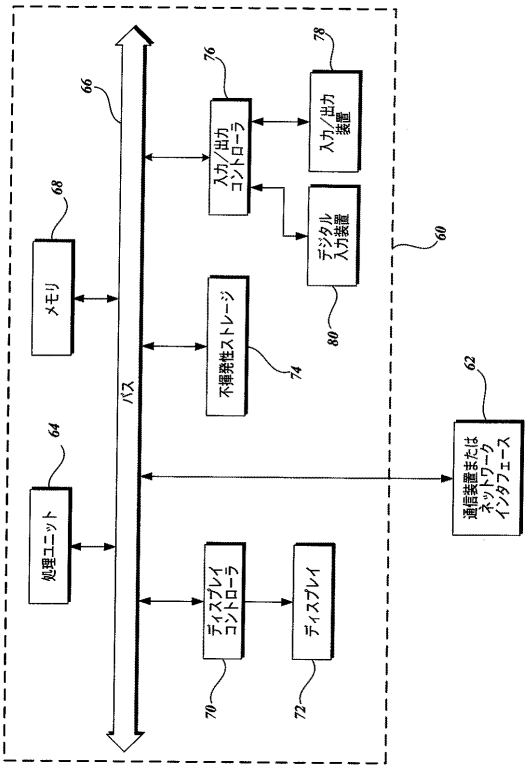
【図４】本発明の例示的な実施形態の動作のシステムレベルの概観を示す図である。

【図５】本発明の例示的な実施形態によるファイルスタンプの例示的なボディを示す図である。
【図６】本発明の例示的な実施形態によるスタンプを含むファイルの作成を示すフローチャートである。
【図７】本発明の例示的な実施形態によるスタンプを含むファイルをスキャンするのに使用することもできるプロセスを示すフローチャートである。
【符号の説明】
【００４１】
３００　ファイルシステム
３０１　ファイル
３０２　アンチウイルスプログラム
３０４　データベースエントリ
３０６　エントリデータ構造ディレクトリ

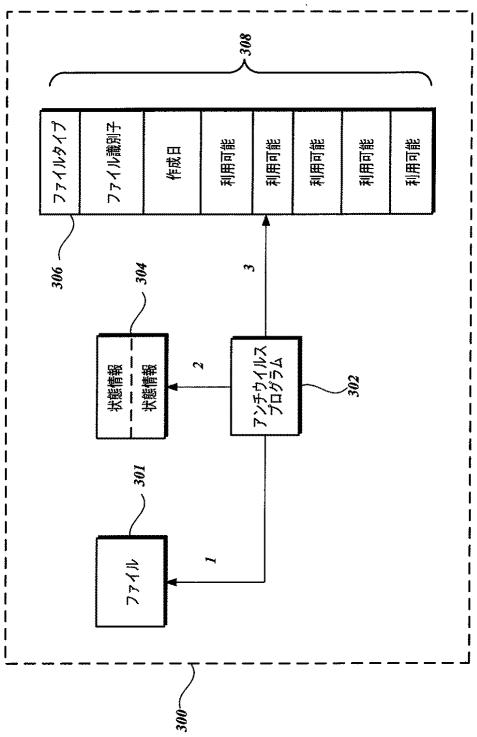
【図１】



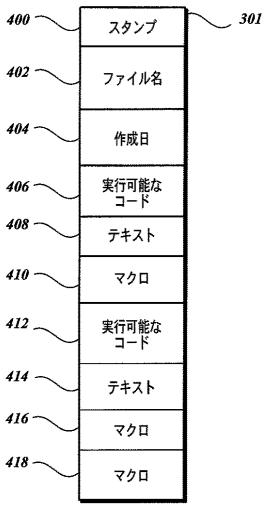
【図２】



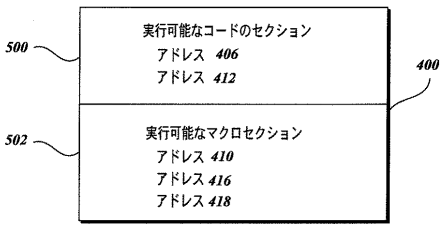
【図３】


308
ファイルタイプ
ファイル識別子
作成日
利用可能
利用可能
利用可能
利用可能
利用可能
306
304
状態情報
状態情報
2
3
アンチウイルス
プログラム
302
301
ファイル
1
300

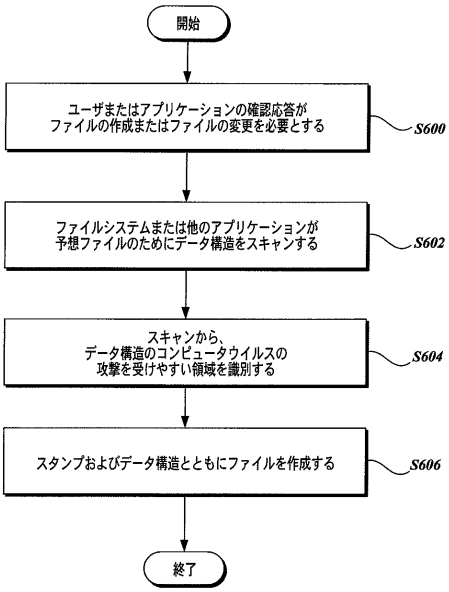
【図４】


400
スタンプ
301
402
ファイル名
404
作成日
406
実行可能な
コード
408
テキスト
410
マクロ
412
実行可能な
コード
414
テキスト
416
マクロ
418
マクロ

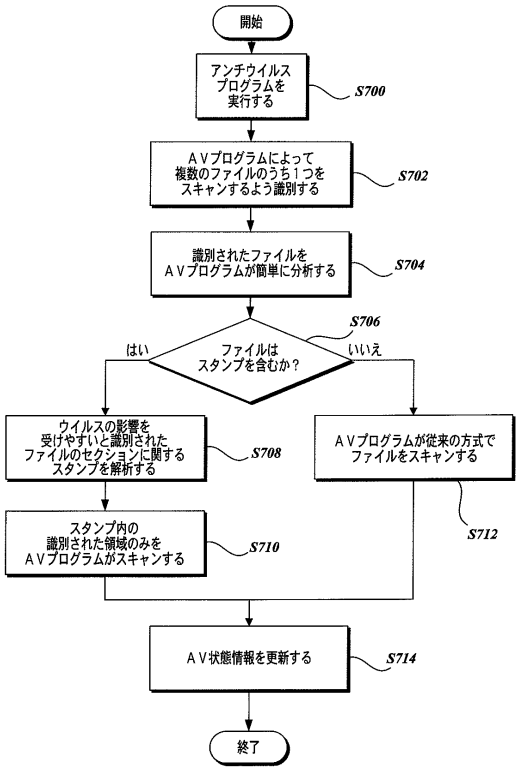
【図５】


500
実行可能なコードのセクション
アドレス 406
アドレス 412
400
502
実行可能なマクロセクション
アドレス 410
アドレス 416
アドレス 418

【図６】


開始
ユーザまたはアプリケーションの確認応答が
ファイルの作成またはファイルの変更を必要とする
S600
ファイルシステムまたは他のアプリケーションが
予想ファイルのためにデータ構造をスキャンする
S602
スキャンから、
データ構造のコンピュータウイルスの
攻撃を受けやすい領域を識別する
S604
スタンプおよびデータ構造とともにファイルを作成する
S606
終了

【図７】


開始
アンチウイルス
プログラムを
実行する
S700
AVプログラムによって
複数のファイルのうち1つを
スキャンするよう識別する
S702
識別されたファイルを
AVプログラムが簡単に分析する
S704
S706
はい
ファイルは
スタンプを含むか？
いいえ
ウイルスの影響を
受けやすいと識別された
ファイルのセクションに関する
スタンプを解析する
S708
AVプログラムが従来の方式で
ファイルをスキャンする
S712
スタンプ内の
識別された領域のみを
AVプログラムがスキャンする
S710
AV状態情報を更新する
S714
終了

フロントページの続き

審査官　後藤　彰

(56)参考文献　特表２００１－５０８５６４（ＪＰ，Ａ）
特開平１０－３３３９０２（ＪＰ，Ａ）
特開２００４－１９９２１３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２２