

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第4652565号
(P4652565)

(45) 発行日 平成23年3月16日(2011. 3. 16)

(24) 登録日 平成22年12月24日(2010. 12. 24)

(51) Int.Cl. F 1
G06F 21/22 (2006. 01) G06F 9/06 660N

請求項の数 1 (全 6 頁)

(21) 出願番号	特願2000-404451 (P2000-404451)	(73) 特許権者	300076633 コグニティブリサーチラボ株式会社 東京都港区六本木7-8-25 永谷リ ード六本木303
(22) 出願日	平成12年12月22日(2000. 12. 22)	(74) 代理人	100096105 弁理士 天野 広
(65) 公開番号	特開2002-196944 (P2002-196944A)	(72) 発明者	苫米地 英人 東京都港区六本木六丁目8番10号 ステ ップ六本木3F東館
(43) 公開日	平成14年7月12日(2002. 7. 12)	(72) 発明者	野口 直夫 東京都港区六本木六丁目8番10号 ステ ップ六本木3F東館
審査請求日	平成19年11月20日(2007. 11. 20)	審査官	後藤 彰

最終頁に続く

(54) 【発明の名称】 抗体接種型動的アンチウイルスシステム

(57) 【特許請求の範囲】

【請求項 1】

実行プログラムに外部モジュールを動的にリンクする動的リンク手段と、
コンピュータウイルスに関する情報やウイルスに対する対応処方であるセキュリティ情
報をネットワーク経由で収集するセキュリティ情報収集手段と、

実行プログラムの実行開始時に前記動的リンク手段を用いて、当該実行プログラムと、
前記セキュリティ情報収集手段により収集されたセキュリティ情報もしくはコンピュータ
が読み込み可能なデータメディアで配布されたセキュリティ情報を基にコンピュータウ
イルスを検出し、コンピュータウイルスへの対抗手段がある場合は当該対抗手段を実行し、
対抗手段がない場合は実行プログラムの実行を取り止めるよう制御するセキュリティ監査
手段として機能させるプログラムと、前記セキュリティ監査手段で利用されるパターンフ
ァイルであって前記セキュリティ情報に基づいて追加されたパターンファイルを含むセキ
ュリティ監査データとを一体化したセキュリティ監査機能付実行プログラムを生成し、前
記実行プログラムの代わりに当該セキュリティ監査機能付実行プログラムを実行させるプ
ログラム起動制御手段と、

を有することを特徴とする抗体接種型動的アンチウイルスシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークに接続されたコンピュータのほか、ネットワーク接続されていな

いコンピュータで外部から情報を読み込む機能を有するコンピュータにおいて、コンピュータウイルスからコンピュータおよびコンピュータ上に保持されている実行ファイル及びデータを保護することが可能である。

【0002】

【従来の技術】

従来、コンピュータウイルスに汚染されたファイルを検出し、コンピュータウイルスへの対抗手段がある場合は対抗手段を実行し、対抗手段がない場合はコンピュータウイルスに汚染されたファイルは利用せぬようにユーザに警告を出すコンピュータウイルスへの対抗ソフトウェアは存在している。しかし、従来のコンピュータウイルスへの対抗ソフトウェアはコンピュータ自身の起動時もしくは一定の時間毎に実行するよう制御されたものである。

10

【0003】

【発明が解決しようとする課題】

このように従来からコンピュータウイルスに対抗するソフトウェアは存在したが、このソフトウェアは常に実行しているとは限らない。ウイルスに汚染されたデータファイル及び実行ファイルを知らずにインターネットから自らのコンピュータにダウンロードしたり、データメディアから自らのコンピュータにコピーしたり、電子メール環境の普及によりメールの添付ファイルという形でウイルスに汚染されたデータがユーザの知らぬ間に自らのコンピュータに入り込むという状況もあり、ユーザは有効な対策を取れないまま、このウイルスに汚染されたデータをアプリケーションプログラムを用いて利用して初めてその被害に気づくという問題がある。

20

【0004】

また、従来のコンピュータウイルスに対抗するソフトウェアは独立したアプリケーションプログラムであるため、このコンピュータウイルスに対抗するソフトウェア開発時に想定されたウイルスに対しては有効な対処を取ることが可能であるが、コンピュータウイルスに対抗するソフトウェア開発後に新たに出現したウイルスなど想定以外のウイルスに対しては全くの無力である。そのため、ユーザは常に新しいコンピュータウイルスに対抗するソフトウェアを入手し実行できる環境を整備する必要があるという問題がある。

そこで発明者らは、鋭意研究をなし下記の発明を為した。

【0005】

30

【課題を解決するための手段】

本発明は、実行プログラムに外部モジュールを動的にリンクする動的リンク手段と、コンピュータウイルスに関する情報やウイルスに対する対応処方であるセキュリティ情報をネットワーク経由で収集するセキュリティ情報収集手段と、実行プログラムの実行開始時に前記動的リンク手段を用いて、当該実行プログラムと、前記セキュリティ情報収集手段により収集されたセキュリティ情報もしくはコンピュータが読み込み可能なデータメディアで配布されたセキュリティ情報を基にコンピュータウイルスを検出し、コンピュータウイルスへの対抗手段がある場合は当該対抗手段を実行し、対抗手段がない場合は実行プログラムの実行を取り止めるよう制御するセキュリティ監査手段として機能させるプログラムと、前記セキュリティ監査手段で利用されるパターンファイルであって前記セキュリティ情報に基づいて追加されたパターンファイルを含むセキュリティ監査データとを一体化したセキュリティ監査機能付実行プログラムを生成し、前記実行プログラムの代わりに当該セキュリティ監査機能付実行プログラムを実行させるプログラム起動制御手段と、を有することを特徴とする抗体接種型動的アンチウイルスシステムを提供する。

40

【0006】

【発明の実施の形態】

本発明の抗体接種型動的アンチウイルスシステムは、動的リンク手段11を有し、アプリケーションプログラム実行時すなわちデータ利用時に必ず実行されるため、ユーザの不注意によるコンピュータウイルスに対抗するソフトウェアの実行し忘れや、ユーザが知らぬ間に自らのコンピュータに入り込んだデータに対しても常にセキュリティ監査手段12

50

が実行されるので、常にコンピュータウイルスからデータを保護することが可能となる。

【0007】

また本発明の抗体接種型動的アンチウイルスシステムは、セキュリティ情報収集手段2もしくはコンピュータが読み込み可能なデータメディアで配布されたウイルス情報を基にセキュリティ監査手段12が実行されるため、常に最新のコンピュータウイルス情報を反映した対処が可能となる。

【0008】

【実施例】

以下図1を参照に本願の抗体接種型動的アンチウイルスシステムについて説明する。

まず本発明の抗体接種型動的アンチウイルスシステムは与えられる環境として、通常のOSならずべてこれを起動できるものである。通常のOSとは、ウィンドウズNT、ウィンドウズ2000、同98、同95、リナックス、ソラリス、BSDなどである。

【0009】

次に、コンピュータウイルスに関する情報やウイルスに対する対応処方をネットワーク経由で収集するセキュリティ情報収集手段2であるが、これはまた、データメディア配布データ5及びインターネット6より情報収集しこれをセキュリティ監査手段12に連結される。

【0010】

ウイルス検知前の段階の当該実行プログラム4は、プログラム起動制御手段13とセキュリティ監査手段12をもってウイルス検知加工され、セキュリティ監査機能付実行プログラム3となる。

ここで、実行プログラム4をA、プログラム起動制御手段13をB、セキュリティ監査手段12をC、セキュリティ監査データをD、セキュリティ監査機能付実行プログラム3をSとしたとき、 $S = A + B + C + D$ となる。そして、Sの部分を生成するために、A、B、C、Dの各要素を一つに結合するための手段が動的リンク手段11なのである。

ここでさらに再度説明を加えると、プログラム起動制御手段13とは検査結果に基づいてプログラムをアボートさせたりするもの、セキュリティ監査手段12とはセキュリティに関わる監査を実行するアルゴリズム的なもの、セキュリティ監査データとはセキュリティ監査手段12で利用されるパターンファイルなどの類である。またこのパターンが刻々変化し、追加されていくため、このデータをさまざまな方法、たとえば、インターネットで収集することになる。これを表現したのがセキュリティ情報収集手段2ということになる。

【0011】

さらにセキュリティ監査機能付実行プログラムを実行する際の流れを表したものが図2及び図3である。即ちセキュリティ監査機能付実行プログラムはまず検査系として、自己検査を為し次に関連ファイルに検査に行くことになる。この検査の結果、検査対象にウイルスが侵入している、或いはファイル内容の破損や改竄などの証拠が見つかった場合、ファイル内容の修復が困難であるならばアプリケーションプログラム本体の起動は危険であると見なして、プログラムを起動不可として実行停止即ちアボートにさせる。

【0012】

【発明の効果】

本発明の抗体接種型動的アンチウイルスシステムを用いることによって、従来のようにコンピュータの起動時もしくは一定の時間毎のみに、侵入したコンピュータウイルスに対処するのではなく、侵入時毎もしくはファイルとしてユーザ自身のコンピュータに取りこまれた時その都度本願の抗体接種型動的アンチウイルスシステムが作動しコンピュータウイルスの対抗手段がある場合は直ちにこの対抗手段を実行させ、これに対処し、対抗手段がない場合はコンピュータウイルスに汚染されたファイルを使用しないように警告を表示するという、ウイルスを水際より撃退させこれを取り込まないという大変効果的な利益をユーザにもたらす。

【0013】

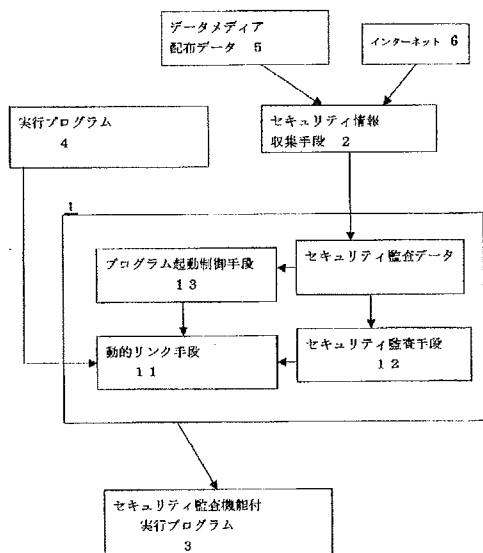
さらに、従来のようにアプリケーションソフトとしての対コンピュータソフトウイルス対抗ソフトのように限られた範囲内のコンピュータソフトウイルスにしか対応できないことはなく、動的リンク手段11及びセキュリティ情報収集手段2もしくはコンピュータが読み込み可能なデータメディアで配布されたウイルス情報を基にセキュリティ監査手段12が実行されるため、想定外のコンピュータソフトウイルスの侵入に対しても汚染されたファイルを使用しないように警告を表示するという、ウイルスを水際より撃退させ、これを取り込まないという大変効果的な利益をユーザにもたらす。

【図面の簡単な説明】

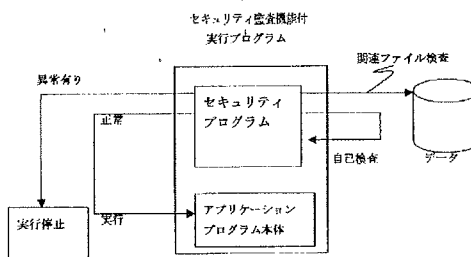
【図1】本発明の抗体接種型動的アンチウイルスシステムの概略構成図である。

【図2】本発明のセキュリティ監査機能付実行プログラムの実行をあらわす概略構成図である。

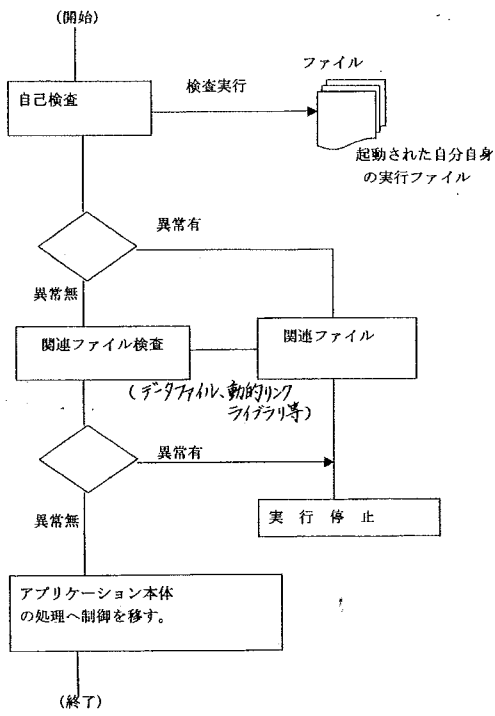
【図1】



【図2】



【図 3】



フロントページの続き

- (56)参考文献 特開平 6-242957 (JP, A)
特開平 6-337781 (JP, A)
特開昭63- 46541 (JP, A)

- (58)調査した分野(Int. Cl., DB名)
G06F 21/22