(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-546111
(P2008-546111A)
(43)公表日　平成20年12月18日(2008.12.18)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660N	5B276
G06F 13/00	(2006.01)	G06F	13/00	610S	

審査請求 未請求　予備審査請求 未請求　（全 27 頁）

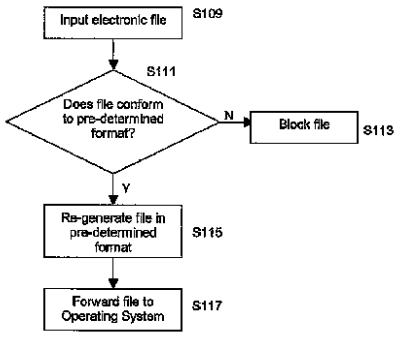
(21)出願番号	特願2008-515291 (P2008-515291)
(86)(22)出願日	平成18年6月9日 (2006.6.9)
(85)翻訳文提出日	平成20年2月7日 (2008.2.7)
(86)国際出願番号	PCT/GB2006/002107
(87)国際公開番号	WO2006/131744
(87)国際公開日	平成18年12月14日 (2006.12.14)
(31)優先権主張番号	0511749.4
(32)優先日	平成17年6月9日 (2005.6.9)
(33)優先権主張国	英国 (GB)

(71)出願人　507402783
グラスウォール・（アイピー）・リミテッド
ＧＬＡＳＳＷＡＬＬ　（ＩＰ）　ＬＩＭＩＴＥＤ
英国エスジー１１・１ビーダブリュー、ハートフォードシャー、ウェア、ハイ・クロス、スタンドン・グリーン・エンド、ブランブル・コティッジーズ２
(74)代理人　100084146
弁理士　山崎　宏
(74)代理人　100081422
弁理士　田中　光雄
(74)代理人　100122286
弁理士　仲倉　幸典

最終頁に続く

(54)【発明の名称】不適切なコードおよびデータの拡散防止

(57)【要約】
所定のデータフォーマットのコンテンツデータを含む電子ファイルを受信する方法またはシステムであって、上記方法は、電子ファイルを受信するプロセスと、データフォーマットを判定するプロセスと、コンテンツデータを構文解析するプロセスとを備えて、上記コンテンツデータが上記所定のデータフォーマットに一致するか否かを判定する。上記コンテンツデータが上記所定のデータフォーマットに一致している場合、上記構文解析されたデータを再生し、再生された電子ファイルは上記データフォーマットで生成される。



【特許請求の範囲】
【請求項１】
一連の規則に対応する所定のファイル形式のコンテンツデータを含む到来電子ファイルを受信する方法において、
上記到来電子ファイルを受信することと、
表明されている所定のファイル形式を判定することと、
上記判定された表明されている所定のファイル形式に対応する一連の規則を備える所定のデータフォーマットに従って、上記コンテンツデータを構文解析することと、
上記コンテンツデータが上記所定のデータフォーマットに一致する場合、上記一致する構文解析されたコンテンツデータを再生して、上記表明されているファイル形式において代替の再生された電子ファイルを生成することと
を備え、
上記代替の再生された電子ファイルは上記再生されたコンテンツデータを含んでいることを特徴とする方法。
【請求項２】
請求項１に記載の方法において、
上記データフォーマットは、各ファイル形式に対して、上記所定の一連の規則の一部に対応していることを特徴とする方法。
【請求項３】
請求項１に記載の方法において、
上記コンテンツデータは、受け入れ可能なデータの既知例に一致するか否かを判定することを備えていることを特徴とする方法。
【請求項４】
請求項３に記載の方法において、
上記データフォーマットは、許可可能な制御文字を含むのみであることを特徴とする方法。
【請求項５】
請求項３に記載の方法において、
上記データフォーマットは、複数のデータ項目を含み、各データ項目は、関連する所定のサイズ限界を有していることを特徴とする方法。
【請求項６】
請求項５に記載の方法において、
上記所定のサイズ限界は、イメージファイル内のラインのサイズであることを特徴とする方法。
【請求項７】
請求項１に記載の方法において、
上記到来電子ファイルをスクランブルフォーマットでメモリに格納することを更に備えていることを特徴とする方法。
【請求項８】
請求項７に記載の方法において、
データの各バイトは、ビットの順序が反転して格納されていることを特徴とする方法。
【請求項９】
請求項７に記載の方法において、
上記データは、受信された各対のデータバイトが反転メモリ順に配置されるように、格納されることを特徴とする方法。
【請求項１０】
請求項１に記載の方法において、
上記電子ファイル内からのコンテンツデータが全て上記所定のデータフォーマットに一致する場合に限り、上記代替の再生された電子ファイルを転送することを更に備えていることを特徴とする方法。

【請求項１１】
請求項１０に記載の方法において、
上記電子ファイルの送信者に関連した上記到来電子ファイルの相手の受信者が上記所定のファイル形式を事前承認しているときに限って、上記コンテンツデータの一部、部分または全体が不一致な場合、上記電子ファイルを送ることを更に備えていることを特徴とする方法。
【請求項１２】
請求項１０に記載の方法において、
上記コンテンツデータの一部、部分または全体が不一致な場合、上記電子ファイルを送ることを更に備え、上記到来電子ファイルの相手の受信者が上記電子ファイルの上記所定のデータフォーマットおよび送信者を事前承認していなく、唯一、受信時に上記相手の受信者は上記電子ファイルを承認することを特徴とする方法。
【請求項１３】
請求項１に記載の方法において、
上記所定のフォーマットに一致しないコンテンツデータを警告テキストに置換することを更に備えていることを特徴とする方法。
【請求項１４】
請求項１に記載の方法において、
上記到来電子ファイルは電子メールであって、上記コンテンツデータが上記所定のデータフォーマットに一致する場合、上記再生された電子メールを相手の受信者に送ることを更に備えていることを特徴とする方法。
【請求項１５】
請求項１４に記載の方法において、
上記代替の再生された電子メールは、電子メールクライアントからハードディスクドライブに送られることを特徴とする方法。
【請求項１６】
請求項１４に記載の方法において、
上記代替の再生された電子メールは、インターネットサーバプロバイダのサーバから電子メールクライアントサーバに送られることを特徴とする方法。
【請求項１７】
請求項１に記載の方法において、
着脱可能なメモリ装置からの上記到来電子ファイルを受信することと、上記代替の再生された電子ファイルをコンピュータ装置に送ることとを更に備えていることを特徴とする方法。
【請求項１８】
請求項１～１７のいずれかに記載の方法を実行するようにしたコンピュータプログラムを含むコンピュータ読取り可能媒体。
【請求項１９】
請求項１～１７のいずれかに記載の方法を実行するための命令を含むメモリ手段を備えていることを特徴とする半導体装置。
【請求項２０】
請求項１９に記載の半導体装置において、
上記半導体装置は、半固定メモリ装置または固定メモリ装置であることを特徴とする導体装置。
【請求項２１】
請求項１９に記載の半導体装置を備えていることを特徴とするネットワークカード。
【請求項２２】
不一致ファイルを拒絶するようにしたコンピュータシステムにおいて、
所定のデータファイル形式のコンテンツデータを含む到来電子ファイルを受信するようにした受信手段と、

表明された所定のデータファイル形式を判定するようにした判定手段と、
上記ファイル形式に関連付けられる所定のデータフォーマットに従って、上記コンテンツデータを構文解析するようにした構文解析手段と、
上記コンテンツデータが上記表明された所定のデータフォーマットに一致するか否かを判定するようにした判定手段と、
上記判定手段の肯定的な判定時に、上記構文解析された一致コンテンツデータを再生する再生手段と
を備え、
上記再生されたコンテンツデータを含む代替の再生された電子ファイルを、上記表明された所定のデータファイル形式にて生成することを特徴とするコンピュータシステム。

【請求項２３】
不一致ファイルを拒絶するようにしたコンピュータシステムにおいて、
所定のファイル形式のコンテンツデータを含む到来電子ファイルを受信するようにしたコンピュータと、
表明された所定のデータファイル形式を判定するようにしたプロセッサと
を備え、
上記プロセッサは、上記ファイル形式に関連付けられる所定のデータフォーマットに従って、上記コンテンツデータを構文解析するようにしたパーサを備え、
上記プロセッサは、更に上記コンテンツデータが上記表明された所定のデータフォーマットに一致するか否かを判定するようになっており、
上記プロセッサは、上記判定手段の肯定的な判定時には、上記構文解析された一致コンテンツデータを再生し、この再生されたコンテンツデータを含む代替の再生された電子ファイルを、上記表明された所定のデータファイル形式にて生成するようになっていることを特徴とするシステム。

【請求項２４】
所定のデータフォーマットのコンテンツデータを含む電子ファイルを受信する方法において、
上記電子ファイルを受信するプロセスと、
上記データフォーマットを判定するプロセスと、
上記コンテンツデータが上記所定のデータフォーマットに一致するか否かを判定するために、上記コンテンツデータを構文解析するプロセスと
を備え、
上記コンテンツデータが上記所定のデータフォーマットに一致している場合、上記構文解析されたデータを再生して、再生電子ファイルを上記データフォーマットにて生成することを特徴とする方法。

【請求項２５】
請求項２４に記載の方法において、
いずれかのコンテンツデータが上記所定のデータフォーマットに一致しない場合、上記所定のデータフォーマットに一致しない上記コンテンツデータは、上記再生電子ファイルに含まれないようにブロックされることを特徴とする方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、不適切なコードおよびデータの拡散を防止するコンピュータシステムと、それらシステムをオペレーションする方法とに関する。

【背景技術】
【０００２】
過去１０年間、コンピュータシステムは、不適切なコードの攻撃を受けることが多くなっている。（現在までの）不適切コードの最も極端な例は、コンピューターウイルスである。コンピューターウイルスは、同名の生物ウイルスのように、１台のマシンに感染し、

次にそこから、電子メールシステムの情報源を乗っ取ることによって、他のコンピュータに感染することができる。その結果、ウイルスが侵入した各コンピュータのアドレス帳を用いて、コンピュータへウイルスを含む電子メールが、１台のコンピュータから他の多くのコンピュータに送信される。

【０００３】

そして、結果的に、帯域幅（回線容量）が浪費され、これがユーザにとって頭痛の種となっている。更に、多くのウイルスは、侵入した各コンピュータにおいて、例えばファイルの消去など、好ましくない動きをする。

【０００４】

ウイルスは、典型的には、別個の添付ファイルで、実行可能なコードとして到来する。しかし、ウイルスは、電子メールの一部に隠されていることもあり、明確なコードの分離や実行をユーザに要求することなく、活動するようになる。ワードプロセッサ、スプレッドシート、データベースなどの多くのアプリケーションには、強力なマクロスクリプト言語が含まれている。マクロスクリプト言語は、ドキュメントのように見えるファイルに、特定の動作を行うことができるスクリプトを含ませることが可能である。ウイルスの作者は、マクロウイルスを書くためにそのようなスクリプト言語を利用し、そして、ドキュメントのように見えるファイルを含んだ電子メール添付物が、隠蔽ウイルスの隠れ場所となる。

【０００５】

ウイルスは、不適切なコードが唯一の形態ではない。「無料」のプログラムが、隠された「スパイウェア」とともによく配布される。スパイウェアは、例えば、ユーザのコンピュータに密かにインストールされる。スパイウェアは、その後、訪れたウェブサイトや他のトランザクションを遠隔のコンピュータに報告する可能性がある。スパイウェアのうちの或るものは、好ましくない広告を表示させる。また、或るスパイウェアは、モデムが高額料金の番号を繰り返しダイアルするようにし向けて、スパイウェアの作者が遠距離通信オペレータから収入を受け取る。その他の有害な種類のコードとしては、マルウェア、ワーム、トラップドアなどがある。

【０００６】

ウイルスが、或るコンピュータから他のコンピュータへと自己増殖する一方で、スパムメール（無差別広告メール）やディスク上での隠れた配布によって、或いは、益々増加する何の気なしに開いたウェブサイトからのダウンロードによって、ウイルス以外の形態の不適切コードが配布されている。この種の不適切コードは、全て共通して、その存在や真の目的が隠匿され、ターゲットとなったコンピュータの所有者やユーザには分からないという事実である。或る種のものは比較的害が少ないが、貴重なビジネスデータを一掃する能力をもつものもあり、これ故に、ウイルス除去ソフトウェアを提供する産業が発展してきた。

【０００７】

現在知られているアンチウイルス（ウイルス駆除）ソフトウェアは、保護されるコンピュータ上で実行されるプログラムから構成される。このようなプログラムは、典型的には、モニタモードとスキャンモードとで動作する。上記モニタモードでは、アクセスされるファイルに対して、そのファイルへアクセスされるたびにウイルスチェックが行われる。上記スキャンモードでは、（ディスクドライブなどの）特定な場所の全てのファイルがスキャンされる。アンチウイルスプログラムのプロバイダは、ウイルスの発生を監視していて、新しいウイルスが検出されると、アンチウイルスプログラム会社は、ウイルスを解析し、ウイルスを検出するのに使用できるデータを抽出する。次いで、このデータは、当該特定のアンチウイルスプログラムを実行するコンピュータが利用できるものとされる。すなわち、上記プログラムは、典型的には、アンチウイルスプログラム会社のウェブサイト上に提供され、ダウンロードすることによって、上記プログラムの実行が図られる。

【０００８】

ウイルスは種々様々な方法で検出される。ウイルスの一部を形成する一連の特徴コード

を保存することができる。また、上記一連の特徴コードの存在に対してスキャンされたファイルを保存することができる。すなわち、上記一連の特徴コードは、ウイルスに対する「サイン」または「指紋」として機能する。これに代わって、ウイルスは、それが意図する挙動によって検出することができる。また、ソースコードやスクリプトファイルを解析して、ウイルスの特徴である所定動作を検出してもよい。

【０００９】

ウイルスは、不幸にも、生物のウイルスと同様、容易に「変化」できる。大文字や小文字の置換に相当するようなコードの小さな変化によって、ウイルスのサインを変化させることができる。したがって、如何なる方法であれ、ウイルスを検出するためのデータファイルは、極めて大きなものとなっている。また、アンチウイルスプログラムに費やされる時間は、チェックすべきサインや規則の数が大きくなるにつれて、それに対応して、増大している。この時間の増大は、ウイルススキャンモードでは許可できるかもしれないが、モニタモードでは、ファイルへのアクセス所要時間に対して、絶えず増加する待ち時間が付加される。更に、ダウンロードがより大きなものとなるにつれて、また、より頻繁に必要になるにつれて、ユーザが必要な最新情報をダウンロードし損なって、したがって、最も新しい（したがって最も危険な）ウイルスに対して無防備となる危険性が高い。

【発明の開示】

【発明が解決しようとする課題】

【００１０】

したがって、本発明は、不適切なコードに抗した保護への全く異なるアプローチを取るものである。本発明の一側面によれば、所定のデータフォーマットのコンテンツデータを含む電子ファイルを受信する方法であって、上記電子ファイルを受信するプロセスと、上記データフォーマットを判定するプロセスと、上記コンテンツデータを構文解析するプロセスとを備え、上記コンテンツデータが上記所定のデータフォーマットに一致するか否かを判定し、上記コンテンツデータが上記所定のデータフォーマットに一致している場合、上記構文解析されたデータを再生して上記データフォーマットにて再生電子ファイルを生成する。

【００１１】

対応するコンピュータシステム、プログラム、およびそのようなプログラムを載せる媒体も提供される。

【課題を解決するための手段】

【００１２】

本発明の一実施形態は、それぞれの受信されたファイルを解析し、次いでそれから代替ファイルを再構成するように動作する。オリジナルファイル自体は保護すべきコンピュータ上に直接保存されたりアクセスされたりしないため、オリジナルファイルはそれ自体ではそのコンピュータに害を及ぼすことはできない。オリジナルファイルは、例えば、それが実行できないビット反転形式その他の形式で保存されるであろう。一方、上記代替ファイルは、「クリーンな」コードおよびデータしか生成することができないジェネレータルーチンを使用して生成される。したがって、受信されたファイル内のコードがどのようなコードであってもそれに対応した不適切コードを生成することはできない。

【００１３】

本発明の一部は、コンピュータファイルに関する幾つかの長く知られている真実の新たな応用にその根拠を置くことができる。最近ではコンピュータにインポートされる大多数のファイルが標準化されたファイルフォーマットである。独自に開発したプログラムは、それら自身のファイルフォーマットを作り出している（そしてそれらのプログラムによって使用されることを予定しているデータはそれらのフォーマットに合致しなければならない）が、異なる独占プログラム間のデータの交換に対しては少なからぬ需要がある。すなわち、第一に、１つの独占プログラムには別の独占プログラムによって書かれたデータを読み込むためのインポートフィルタがたいてい供給されており、第二に、如何なる独占プログラムにも関連づけられていない幾つかのフォーマットが存在する。そのような汎用的

なフォーマットの例としては、ＡＳＣＩＩテキスト、リッチテキストフォーマット（ＲＴＦ）、ハイパーテキストマークアップランゲージ（ＨＴＭＬ）、およびエクステンシブルマークアップランゲージ（ＸＭＬ）がある。

【００１４】

したがって、ファイル中のデータは、それが任意のアプリケーションプログラムによって読み込まれることになっており、かつ様々なファイルで使用される各フォーマットが広く知られているものであるならば、厳格な規格に精確に従っていなければならない。本発明者らは、各ファイルによって使用される各フォーマットは幅広く変化することを許可しているが、大多数のファイルには幾つかの比較的狭い実用的な制約を満たすデータが含まれているということに気づいた。例えば、ほとんどのオペレーティングシステムおよびアプリケーションは、かなりの長さのファイルタイトルを受け入れるが、ほとんどのユーザが、たいてい短くて容易に認識できるファイル名を使用する。

【００１５】

したがって、本発明の一実施形態によって行われる解析は、表明されたファイル形式の仕様にそれ以外では一致しているデータが、実用的な限界に違反しているか否かを検出することを含むものとすることができる。これらの「現実世界」の制約は、本発明が「正常な」受け入れ可能なファイルを検出することを可能にする。このタイプの実用的な限界に対応していない如何なるファイルコンテンツもジェネレータプログラムに渡されることはなく、したがってユーザのコンピュータに実行可能な形式において到達することはない。

【００１６】

したがって、本発明の一実施形態は、周知のアンチウイルスプログラムとは基本的に異なった様式で動作するものであることが分かるであろう。周知のアンチウイルスプログラムは、ウイルスを検出することを狙いとしており、ウイルスであることが検出されない全てのものを通過させる。したがって、それらのプログラムは最大の危険から、すなわち未知のウイルスの危険からユーザを保護することに必ず失敗する。新参のウイルスはそれぞれ、ウイルス対策会社の注目するところとなる前に、既に多くのコンピュータに感染してしまうに違いない。

【００１７】

更に、ウイルス対策ソフトウェアがインストールされ、検出済みデータの最新版を保有している場合でも、ウイルスは、そのウイルス対策ソフトウェアによって検出可能となる前に、通常、保護されるコンピュータのハードドライブその他の媒体に保存されるであろう。何らかの理由でウイルス対策ソフトウェアが動作しないと、そのウイルスは適当な場所にあって活性化される可能性がある。

【００１８】

公開米国特許出願ＵＳ２００３／０１４５２１３は、ファイル内においてマクロまたは悪意のあるコードを検出するシステムを開示している。そのファイルは、その後、テンプレートで再構築され、その悪意のあるコードがテンプレートから除去されて、上記ファイルの汚染されていないバージョンを提供する。

【００１９】

全く対照的に、本発明は、ウイルスを検出することも、また代表的なウイルス様の挙動を拒絶することすらも、その狙いとする必要がない。その代わりに、全ての入力ファイルを完全に拒絶することができ、可能な場合はそれらのファイルを、不適切なコードおよびデータを含ませることができない生成ファイルに代替させる。したがって、不適切なコードおよびデータが、保護すべきコンピュータのハードドライブに実行可能な形式で到達することを防ぐことができ、それらが１台のコンピュータから別のコンピュータへ伝染することは不可能となる。

【００２０】

ここで、公開米国特許出願２００３／２２９８１０が、ウイルスに対する保護策として「光学式ファイアウォール」の提案を開示している。この後すぐに明白になるであろう理由により、このシステムは実施に移された（または、実施に移すことができたものである

）とは考えられない。その公開出願には、ファイアウォールコンピュータが画像ファイルなどのファイルを受け取って、そのファイアウォールコンピュータのディスプレイ上にその画像を表示するシステムが記載されている。光学式センサアレイが画像をスキャンし、スキャンされた画像が相手の受信者に与えられる。画像内に隠されたウイルスはどれも表示されず、したがってスキャンされた画像においてウイルスであるとは判定されない。変形例として、スクリーンのビットマップを実際のスクリーン表示の代わりに使用する場合もある。

【００２１】

様々な理由から、上述の米国特許出願において提供される「光学式カプラ」ファイアウォールは、ウイルスに対する有効かつ信頼できる保護を提供することはできないであろう。

【００２２】

例えば、光学式文字認識（ＯＣＲ）ソフトウェアを使用した再現は、不適切な情報を提供する可能性がある。更に、ビデオ技術を使用した画像の再現は、意図したより低い品質の画像を提供する可能性がある。また、入力ファイルがウイルスを含む場合、その入力ファイルを受信するコンピュータが感染してしまうであろう。

【００２３】

他方、再生ファイルを実行し、表示し、光学スキャンする代わりに、それらのファイルを解析し、次に、再生することにより、本発明の一実施形態は、大多数の場合、オリジナルファイル（それに不適切コードがないならば）と匹敵する代替ファイルをその代替が透明になるようなしかたで提供することができる。

【００２４】

ファイルフォーマットは、それらの複雑さにばらつきがある。一方の極において、テキストファイルは単純なフォーマットを有する。スクリプトやマクロを含むことができるファイル（ワードプロセッサやスプレッドシートファイルなど）は、中間的な複雑さのものであるが、コードを含むファイルはコードパーサ（コード構文解析ツール）によってしか完全に解析することができない。本発明によればそのようなコード解析は結局可能となるが、本発明の実施形態は、その１つの利便性として、ドキュメントファイルから全てのマクロとスクリプトを除去し、プログラム、コード、マクロまたはスクリプトだけから成る如何なるファイルも通過させないように動作することもできる。

【００２５】

ユーザが上記のようなファイルを受信することを望む場合も頻繁におこるであろうことは容易に想像がつく。したがって、１つの好ましい実施形態においては、本発明は、特定のソースに由来するファイル（または特定の形式のファイル）は常時通過させ、他のソースに由来するファイルは拒絶するように、ソースによってファイルをフィルタリングするように構成したフィルタと同時並行で動作するようにしてもよい。

【００２６】

このように、本発明の実施形態は全てのソースからのファイル内のコードを受信することをブロック（阻止）する一方で、並列フィルタが既知のソースからだけの上記ファイルを許可する。したがって、ユーザは、本発明によって拒絶されるであろう、例えば、システム管理者や公認されたウェブサイトからのファイルを受信することができる。ユーザがコードを受信することを望むそれらのソースのみを識別することにより、本発明は不適切コードを阻止することができる。

【００２７】

本発明はウイルスを検出することより、むしろファイル規格との一致および代表的なユーザの対応を検出することによって機能することが可能となるため、頻繁な更新は不要である。そのような更新が必要となるのは、ある規格に対する大きな変更が広範囲に受け容れられたとき、あるいはユーザの対応が実質的に変化したときだけであり、これらはいずれもウイルス対策の更新版を配布しなければならないときの大急ぎのスピードと比べるとスローな処理過程である。同様に、実行すべきテストの回数が時間の経過とともにほぼ安

定して維持されるため、プログラム起動のための待ち時間も時の経過によって全く増加しない。

【００２８】

本発明のこれらおよびその他の側面、実施形態および利点について次の記載および請求項において論ずる。ここで、本発明の実施形態を添付の図面を参照して説明するが、これは例示として説明するに過ぎない。

【発明を実施するための最良の形態】

【００２９】

第１実施形態

本発明の第１実施形態を示す基本的システムレイアウトは、図１Ａに示される。電子ファイル１０１は、情報源（ソース）で生成され、伝送媒体１０３を介して伝送される。伝送媒体１０３としては、有線システムや無線システムなどの電子ファイル伝送に適した媒体を用いることができる。電子ファイル１０１は、通常の方式で伝送媒体１０３を通過して送信先に到達する。本実施形態では、ＡＶ（アンチウイルス）アプリケーション１０５が送信先のシステムにインストールされている。ＡＶアプリケーション１０５の動作によって、到来する電子ファイル内のデータは、予め定義された許可フォーマットに照らして解析されるまで、送信先のオペレーティングシステム１０７への進入が許可されず、また、データが許可されるものであると判定された場合には、再生される。すなわち、ＡＶアプリケーション１０５は、電子ファイル１０１がオペレーティングシステム１０７に通過許可できるか否かを決定するものである。

【００３０】

図１Ｂは、本発明の実施形態を実施するのに一致したコンピュータシステムを示す。コンピュータ１０９は、入力インタフェース１１１において、到来する電子ファイル１０１を受信する。入力インタフェース１１１はマイクロプロセッサ１１３に接続されている。マイクロプロセッサ１１３は、受信されたファイルに対して、様々なプロセスを実行するように構成されている。マイクロプロセッサ１１３はパーサ（構文解析ツール）１１５を含んでいる。マイクロプロセッサ１１３は、更に、メモリ装置１１７と、ディスクドライブ１１９と、ディスプレイ１２５やキーボード１２７などの出力装置への接続を可能にする幾つかのインタフェース（１２１、１２３）とに接続されている。

【００３１】

到来した実行可能なファイルがＡＶアプリケーション内に入ったときに自動的に実行されることがないように、本システムでは、到来する電子ファイルを構成するデータを、何らかの適切なスクランブル（暗号化）フォーマットで、メモリに格納するようになっている。

【００３２】

この実施形態では、スクランブル法によって、１バイト内のビットの順序が反転されている。すなわち、ビット０～７は順序通りに受け取られるが、ビット反転方式で格納され、ビット０がビット７に転換され、ビット１がビット６に転換され、ビット２がビット５に転換され、ビット３がビット４に転換される。したがって、例えば、１０１１００００から成る１バイトの場合、００００１１０１の順序で格納される。このようにして、如何なる実行可能なコードも自動的に実行されることが不可能となり、したがって、如何なる既感染電子ファイルもＡＶアプリケーションまたは送信先のオペレーティングシステムに感染することができない。

【００３３】

ファイルの所望の送信先にＡＶアプリケーションを配置する代わりに、ＡＶアプリケーションを情報源に、或いは、伝送媒体内の何処かに配置してもよい。或いは、電子ファイルを伝送経路に沿った地点で解析することが可能であるならば、それ以外の場所に配置してもよい。

【００３４】

図１Ｃは、電子ファイル１０１が送信先のオペレーティングシステム１０７への通過が

許可されるか否かを決定すべく、第１実施形態においてＡＶアプリケーション１０５が実行する基本ステップのフローチャートを示している。ステップＳ１０９では、電子ファイル１０１が、任意の適切な手段を用いて、ＡＶアプリケーション１０５に入力される。この入力手段は、受け取られる電子ファイルの種類と、電子ファイルが伝送される媒体とに依って、変えることができる。この実施形態においては、電子ファイル１０１はＡＶアプリケーション内に受け入れられる。

【００３５】

ステップＳ１１１では、電子ファイル１０１が所定のフォーマットに一致しているかどうかを判定すべく、一致解析装置によって解析が行われる。ＡＶアプリケーションは、既知で許可可能な予め定義された複数の格納済フォーマットのうちの１つに一致する電子ファイルのみを通過できるように、設計されている。一般に、ファイルはコンテンツデータから構成される。上記コンテンツデータは、特定の一連の規則から成るファイル形式の仕様にしたがって符号化され配列される。ファイルの各形式（テキスト、ＨＴＭＬ、ＸＭＬ、スプレッドシートなど）は関連する一連の規則を有する。一般的なファイルの形式は、屡々、ファイル名の末尾語（例えば、.ｐｄｆや.ｔｘｔや.ｄｏｃ）によって示される。或いは、それに代わって、ファイル中の初めの数バイトのデータによって示されることがある。ファイルの形式の多くは、ファイル構造に関するものを示すヘッダを含み、次にコンテンツデータ（例えば、テキスト、数字、音声または画像のデータ）が続く。

【００３６】

コンテンツデータは、パラメータ（例えば、コンテンツデータがボールド体で表示されることを示すタグ）を含んでもよい。ファイル形式の仕様を構成する規則は、そのようなパラメータが取ることのできる値や範囲を指定するものとしてよい。それらの規則は、例えば、コンテンツデータが取り得る許可値または許可範囲値を指定するものとしてもよい。

【００３７】

特定の形式のファイルを開くことができるアプリケーションプログラムは、ファイル形式の仕様を構成する規則をファイルに適用するために、パーサ（構文解析ツール）を含んでいて、コンテンツデータを抽出して表示または処理する。例えば、ワードプロのアプリケーションは、ファイルを、その工業所有権が保護されたファイルフォーマット（例えば、登録商標Ｍｉｃｒｏｓｏｆｔ Ｗｏｒｄ）で開くことができる。また、その他のワードプロのアプリケーションの所有権保護されたファイルフォーマットでファイルを開くことができるし、リッチテキストフォーマット（ＲＴＦ）やＡＳＣＩＩやＨＴＭＬなどの一般的なファイルフォーマットでも、ファイルを開くことができる。特定の形式のファイルとしてコンテンツデータを格納できるアプリケーションプログラムは、ファイル形式の仕様を構成する規則をコンテンツデータに適用するためのジェネレータを含んで、ファイルを所要のフォーマットで作成する。

【００３８】

本実施形態では、各ファイル形式に対して、所定のフォーマットが格納されている。この所定のフォーマットは、通常、そのファイル仕様を構成する規則を含んでいる。しかし、所定のフォーマットは、頻繁に使用されるフォーマット（の一部分）に関連した規則を含んでいるに過ぎない。更に、所定のフォーマットは、一般的かつ頻繁に使用される値と範囲を含むだけのものとなるように、追加規則を含んで、コンテンツおよびパラメータが取り得る数値や範囲を制約する。このようにして、所定形式のファイルの一部分は、頻繁に日常的に発生するデータとパラメータとから専ら成り、本実施形態の対応する格納済所定フォーマットによって、上記ファイルの一部分のみを解析することができる。

【００３９】

システムを通過するのを許可されないデータ形式の構成要素の例としては、ワードプロセッサで作成されたファイル中の複合マクロや、ＨＴＭＬ頁中のＩフレームがある（上記データ形式は稀にしか使用されないので、それらに関する規則を所定のフォーマットが含んでいなく、したがって許可されない）。稀にしか使用されなくてシステムを通過するこ

とが許可されないデータ値の例としては、一般的に使用されるＴＡＢ、ＣＢ／ＬＦ、およびＬＦ文字以外には、ＡＳＣＩＩファイル内の制御文字がある（所定のフォーマットは上記データ値を除外した値に限定される）。

【００４０】

一致解析装置は、電子ファイルが、そのファイル中に記述されているフォーマットに沿うものであるか否かを判定する。また、一致解析装置は、全パラメータが、その特定の電子ファイル形式に関連付けられる所定フォーマットに一致しているかを判定する。電子ファイルがいずれの所定フォーマットにも一致しない場合、電子ファイルは、再生されることなく、ステップＳ１１３において有効にブロックされ、好ましくは消去される。しかし、電子ファイルが所定フォーマットに一致している場合は、コンテンツデータが電子ファイルから抽出され（かつ、データ構造に暫定的に保存され）、ステップＳ１１５に示すように、上記コンテンツデータは、電子ファイル形式に付随した所定フォーマットで（暫定データ構造から）一致解析装置によって再生され、代替ファイルが作成される。

【００４１】

再生された電子ファイルは、次に、ステップＳ１１７で、例えばオペレーティングシステムに送られ、標準の方式で処理される。所定フォーマットを構成する規則を用いてファイルから抽出できるコンテンツデータは、全て、抽出され、再生される。したがって、抽出できない部分は、如何なるものも再生することができない。

【００４２】

このように、ファイルの一致チェックと再生によって、ウイルスがオペレーティングシステムに進入して感染するのは不可能となる。実際、通常見られるフォーマットのコンテンツデータ以外には、抽出されて再生されるものはない。

【００４３】

電子メッセージをサブパーツ（下位部分）に分解することができる状況では、電子メッセージのサブパーツの或るものは所定フォーマットに一致し、それ以外のサブパーツは一致しない。このような状況において、ＡＶアプリケーションは、一致する全てのサブパーツが実在テストに一致するか否かを判定し（例えば、大多数の或いは最重要なパーツが一致するか否かを判定し）、一致する場合は、一致している電子メッセージのサブパーツを再生する。

【００４４】

メッセージの一致しないサブパーツは再生されない。その代わりに、ＡＶアプリケーションは、関連の警告テキストを電子メッセージに挿入して、メッセージの一部が通過許可されないことを受信者に知らせる。選択肢として、この警告テキストは、サブパーツが通過許可されない理由を示すものとすることができる。

【００４５】

更に、電子ファイルのサブパーツの一部分も、この一部分に対応する所定の許可フォーマットに一致していない場合には、ブロックでき、すなわち再生することなく、好ましくは消去できる。すなわち、例えば、ＡＳＣＩＩ電子ファイルの文字列が制御文字（例えば「ＢＥＬ」文字）を含んでいる場合、この文字列を、ＡＶアプリケーションにより挿入されるテキスト警告に置き換えて、この文字列は所定フォーマットに一致しないので再生電子ファイルのこの部分から除外されている、と受信者に知らせることができる。上記一致解析装置は、許可されない制御文字（例えば「ＢＥＬ」文字）を特別に探索するのではなく、所定の許可フォーマットによって定義された許可される制御文字だけを通過させる。

【００４６】

他の方法として、一致しない制御文字は、スペースに置き換えたり、或いは完全に除外したりすることも可能である。種々の選択肢は、例えば、ＡＶアプリケーションが作動する環境に依って、また、少なくとも最小限の一致情報がＡＶアプリケーションを介して目的とする所に至ることが如何に重要かに依って、選択される。

【００４７】

ここで、第１実施形態のさらなる代替を説明する。電子ファイルまたはそのサブパーツ

が一致しなく、したがって目的のオペレーティングシステムに通過到達できないとＡＶアプリケーションが判定する場合、オリジナルの電子ファイルは脅威フィルタアプリケーションへと通される。この脅威フィルタアプリケーションは、電子ファイルまたはそのサブパーツに付随した脅威が存在するか否かを判定する。

【００４８】

この判定は、システムが特定のソースから何を受け取ることを期待しているかに基づいて、行われる。システムは、この判定を、データ形式のリストをメモリに格納された所定のソースリストに照らして吟味検討する。そして、データ形式がそのソースから受け取られるか否かを調べる。すなわち、電子メールがソースによりフィルタリングされているか否かを調べる。したがって、不一致データが脅威でないことが知られている場合、不一致データを含むファイルが同一ソースから受け取られると、オリジナルの不一致データはオペレーティングシステムに通過到達することが許される。このようにして、ＡＶアプリケーションと脅威フィルタアプリケーションとを備えるシステムは、大多数の安全な電子ファイルが所望の送信先に通過到達することを可能とする。

【００４９】

第２実施形態

以下に説明する第２実施形態では、電子ファイルとは、インターネット上で作成者からインターネットサービスプロバイダ（ＩＳＰ）に伝送される電子メールのことである。ＩＳＰは、各電子メールを電子メールクライアントサーバに送る。電子メールクライアントサーバは、電子メールを受信すると直ぐに、相手の受信者の受信ボックスに電子メールを送る。

【００５０】

図２は、本発明のＡＶアプリケーションが組み込まれた本実施形態による電子メールシステムの配置を示す。電子メールは送信者によってソース場所２０１から送信される。その電子メールは、インターネット２０３を経由して、インターネットサービスプロバイダ（ＩＳＰ）２０５へ送られる。上記ＩＳＰは、電子メールに組み込まれたドメイン名によって決定される。受信者の電子メールクライアントサーバ２０７は、ダイレクトオープン接続によって、ＩＳＰ２０５に接続されている。第１の接続は、送信電子メールを電子メールクライアントサーバ２０７からＩＳＰ２０５へ送るためのシンプルメール転送プロトコル（ＳＭＴＰ）送信接続２０９である。第２の接続は、ＩＳＰ２０５から電子メールを取り出すＰＯＰ（ポストオフィスプロトコル）の受信接続２１１である。

【００５１】

ＡＶアプリケーション１０５はＩＳＰ２０５に配置されている。ＡＶアプリケーション１０５は、受信者の電子メールクライアントサーバ２０７に接続された入出力ポートに存在して、電子メールクライアントサーバ２０７によって送受信される全ての送受信電子メールを解析する。

【００５２】

本実施形態では、ＡＶアプリケーション１０５は一片のコンピュータコードである。上記コンピュータコードは、既知のコンピュータプログラミング技法を用いて実行される。電子メールが電子メールクライアントサーバ２０７に入る前に、電子メールクライアントサーバ２０７に送られる電子メールは全て、ＡＶアプリケーション１０５を通過しなければならない。同様に、電子メールクライアントサーバによってＩＳＰ２０５に送られる電子メールは全て、ＩＳＰ２０５に入る前に、ＡＶアプリケーション１０５を通過しなければならない。

【００５３】

ＡＶアプリケーション１０５は、データがこのアプリケーションに入る際に、そのデータを解析することによって、受信電子メールのメッセージを分析する。第１実施形態と同様、実行可能なファイルを動作停止させるべく、データはスクランブルモードで格納されている。ＡＶアプリケーション１０５は、受信電子メールの個々のパーツが所定の許可フォーマットに一致するか否かを判定する。そのパーツが一致する場合は、ＡＶアプリケー

ション１０５は電子メールメッセージの各パーツを再生する。したがって、如何なる電子メール内の如何なるウイルスも、受信者のシステムに感染することは許されなく、また、受信者のシステムからＩＳＰに通ることは許されない。

【００５４】

本実施形態では、一致解析装置は、特定のデータ形式を解析するために用いられていて、（第１実施形態で説明したように）そのデータ形式に対応した所定フォーマットに一致するか否かを調べ、そして、一致するコンテンツデータを抽出する。次に、一致解析装置は、そのデータ形式に対応した所定の許可フォーマットを用いて、そのデータを再生する。各データ形式は、それ自身の特有の一致解析装置によって解析され、再生される。

【００５５】

各一致解析装置は、受け取ったデータに応じて、データに関する特定の規則群を実行する。これらの規則は、ファイル形式に対する所定の公的な仕様によって定義されている。また、現実の世界でよく見られる（したがって安全な）周知のデータ形式の例によって定義されている。上記規則は、一般的に、ファイル形式仕様に一致するファイルのサブセットのみを許可する。しかし、公的仕様の規則の内の或るものは、通常は規則に反するが、緩和することができる。例えば、電子メールアドレスはスペースを含まないが、人気の電子メールアプリケーションにはこの規則を破るものがある。この点に関して仕様に違反する電子メールは、どこにでもある。したがって、本実施形態による電子メールを解析する所定フォーマットは、スペースを含む電子メールアドレスを受け入れて、電子メールアドレスを解析、抽出する。

【００５６】

また、一致解析装置は、データファイル内の特定のパラメータをチェックするものでもよい。例えば、ファイルがＲＴＦ（リッチテキストフォーマット）ファイルであるとヘッダに記述されている場合、最初の数バイトのデータが読み込まれて、これが正しいかどうかを判定する。

【００５７】

図３は、本実施形態に従ってＡＶアプリケーションを組み込んだシステムの動作法のフローチャートを示す。図３に見られるように、ステップＳ３０１において、電子メールが、ＳＭＴＰ受信接続を介して、ＩＳＰ（インターネットサービスプロバイダ）にて受信される。

【００５８】

ステップＳ３０３において、プロトコル一致解析装置が、受信電子メールの基本フォーマットを読み込むプロセスを実行する。そして、基本電子メールプロトコルに一致するように電子メールを再生する。（不一致型の電子メールリーダは電子メールを読む。）次いで、読み込まれたデータは、基本電子メールプロトコルに一致する電子メールライタに渡される。このようにして、何処にでもある不一致は一致電子メールに変換される。例えば、受信者の電子メールアドレスが酷い状態に形成されている場合には、電子メールライタがそれを書き直して一致させる。

【００５９】

もう一つの例は、電子メールメッセージが、「Ｆｒｏｍ：」というヘッダが無い状態で、受け取られるときである。この場合には、電子メールメッセージがカプセル化されて、全体が、ヘッダ「Ｆｒｏｍ：」を含む新しい電子メールメッセージとなる。

【００６０】

電子メール内の他のパラメータも一致したものにされる。上記パラメータは、例えば、行長、正しいＡＳＣＩＩ文字列の使用、適切な場合における正しいＢＡＳＥ６４コーディングの使用、完全なヘッダ情報（「Ｔｏ：」、「Ｓｕｂｊｅｃｔ：」など）、電子メールのヘッダと本文との間のスペースなどである。

【００６１】

電子メールが、その一部を書き直すことができない程に、まずく形成されている場合、不一致部分が脱落しても筋の通る電子メールがまだ存在しているかどうかが判定される。

その処理の結果、まだ電子メールが筋の通ると判定された場合、電子メールは、不一致部分が欠けた状態のままで書き直されることができる。その場所には、警告テキストを挿入してもよい。

【００６２】

また、プロトコル一致解析装置は、電子メール全体を拒絶するものとしてもよい。例えば、プロトコル一致解析装置が、不一致ＢＡＳＥ６４のコード化が電子メール内の大きいデータ片で使用されていることを検出した場合、その電子メールは、ステップＳ３０５において、完全に拒絶される。

【００６３】

プロトコル一致解析装置が、電子メールが電子メールプロトコルに一致すると判定した場合、その電子メールはプロトコル一致解析装置によって再生される。そして、そのプロセスにおいて、次のステップに渡される。

【００６４】

全ての電子メールは、電子メール用の最新ＲＦＣ規格（すなわち、ＲＦＣ８２２とその後続版）に一致させるべきである。この規格は、電子メールがいかに形成されるかを定義している。電子メールがプロトコル一致解析装置を通した後には、ＲＦＣ８２２規格の一致解析装置は、電子メールがＲＦＣ８２２規格に一致しているかどうかを検査する。すなわち、ＲＦＣ８２２規格の一致解析装置は、まず、（後述するように）電子メール内の境界を見つけて電子メールを個々の構成部分に分解し、次に、電子メールの各構成部分を解析してそれがＲＦＣ８２２に一致するかを検査することにより、上記一致チェックを行う。

【００６５】

ＲＦＣ８２２規格の一致解析装置が、周知の全データ形式の一致をチェックできることを保証すべく、ＲＦＣ規格が更新される際には、更新が必要であることが理解される。

【００６６】

周知のごとく、電子メールは、例えば図４に示すように、幾つかの別々の部分から構成される。電子メールは、ＲＦＣ８２２ヘッダ４０１から始まる。ＲＦＣ８２２ヘッダ４０１は、「Ｆｒｏｍ：」、「Ｔｏ：」、「Ｓｕｂｊｅｃｔ：」などの幾つかのフィールドが定義される。その次は、ＭＩＭＥヘッダ４０３である。ＭＩＭＥヘッダ４０３は、「コンテンツ形式」などの拡張プロトコルで使用される幾つかのフィールドを定義する。上記拡張プロトコルは、電子メールの異なる部分間の境界を示すのに使用されるテキストを定義する。

【００６７】

ヘッダ４０１に続いて、最初の境界４０５が示される。電子メールの次の部分は、もう１つのヘッダであるＭＥＶＩＥヘッダ４０７から始まる。ＭＥＶＩＥヘッダ４０７は、この部分で使用されるフォーマットを定義する。この例では、この部分は、テキストフォーマットで表示されるテキスト内容を備える。したがって、その後には、テキスト４０９のブロックが続く。テキストブロック４０９の終わりには、もう１つの境界４１１が存在する。

【００６８】

もう１つのＭＩＭＥヘッダ４１３が、電子メールの次の部分がどのフォーマットであるかを示す。この例では、電子メールの次の部分は、混合テキストおよびＨＴＭＬのフォーマットブロック４１５である。もう１つの境界４１７は、その部分の終わりを電子メールに示す。

【００６９】

電子メールの最後部分として、最終ＭＩＭＥヘッダ４１９が、電子メールの添付物に関するデータ形式を示す。この場合は、上記データ形式はＺＩＰファイルである。ＺＩＰファイル４２１は、符号化されて電子メールに加えられるＢＡＳＥ６４である。次に、最終境界４２３が電子メールの終わりを示す。

【００７０】

図３のステップＳ３０７において、ＲＦＣ８２２規格の一致解析装置は、パーサ（構文解析ツール）を用いて、電子メールを構成するＡＳＣＩＩ文字を解析する。次いで、ＲＦＣ８２２規格の一致解析装置は、電子メールにおける境界を検出して、特定のパラメータが既知の許可可能な所定フォーマットに一致するか否かを検査できる。例えば、ＲＦＣ８２２規格の一致解析装置は行長を検査して、行長がＲＦＣ８２２規格に一致するか否かを調べ、２０００以下の行長のみが再生される。

【００７１】

電子メール内の構文解析されたデータがＲＦＣ８２２規格に一致するか否かを調べるために、更なる検査を行うことができる。例えば、電子メール内の文字が規格で定義された既知の許可可能なＡＳＣＩＩ文字であるか否か、ヘッダ情報が規格で定義された通りか否か、そしてヘッダ長が規格の定義に一致するか否か、が検査される。ここに挙げたこれらの検査は、ＲＦＣ８２２規格の一致解析装置が実行する様々な大検査群の単なる例に過ぎない（その他の部分は、当業者には明白であろう）。本発明は、それ自体、上に挙げた例に限定されるものではない。

【００７２】

ＲＦＣ８２２規格の一致解析装置は、構文解析されたデータを解析して基本ＲＦＣ８２２規格に一致するか否かを調べると同時に、特定のパラメータがＲＦＣ８２２規格の電子メールの現実の例に一致するか否かをも検査する。すなわち、特定のパラメータの仕様では、ユーザが定義するように開放されているが、現実の世界では、妥当な値のみが使用される。例えば、電子メールは、通常、最小の数のパーツを備えるのみである。したがって、１０００個の境界を含む電子メールが受信される場合、この電子メールは、ＲＦＣ８２２規格の電子メールの現実例とはならず、したがってＲＦＣ８２２規格の一致解析装置によって、ブロックされる。すなわち、電子メールは再生されず、好ましくは消去される。

【００７３】

更なる一致チェックを要するデータを含んだ電子メールの各構成部分に対しては、本実施形態では、ステップＳ３０９において、構成部分の対応するデータ形式に依って、構成部分を個別の一致解析装置に送る。すなわち、解析された電子メール部分がテキストと定義された場合、テキストを構成するＡＳＣＩＩ文字が、テキスト一致解析装置に送られる。解析された電子メール部分がＴＩＦＦファイルと定義された場合は、ＴＩＦＦファイルを構成する文字がＴＩＦＦ一致解析装置に送られる。

【００７４】

ステップＳ３０９において、各一致解析装置は、送られてきたデータを解析して、データが、表明されたフォーマットに一致するか否かを調べる。一致する場合、データは一致解析装置によって再生される。データ内に何らかの不一致がある場合、データは一致解析装置によって除外されるか、或いは、可能ならば、一致するようにデータが再生される。データを一致するように再生する例の一つは、入れ子ブラケットが欠けている場合に、ＲＴＦファイルに入れ子ブラケットを追加する例である。

【００７５】

電子メールが異なるデータ形式の入れ子構造を含んでいる場合、一致解析装置が繰り返し呼び出される。そして、数台の特定の装置は順次動作され、各装置は、新たなデータ形式が発見される各ポイントで、待機させられる。このようにして、電子メールは、ＪＰＥＧ写真ファイルを含むワードプロセッサドキュメント等のＺＩＰファイルを帯同するが、一連の異なる一致解析装置（ｚｉｐ、ワードプロセシング、ＪＰＥＧ）を通過でき、入れ子構造のファイルを介してドロップダウンして、各ファイルが順次解析される。解析の終わりには、一致する再生部分を用いて、ファイルが再編成される。

【００７６】

ステップＳ３１１において、適切に理路整然として理解可能かつ有意義な電子メールを形成すべく電子メールの十分な部分が再生されていると判定されると、ステップＳ３１３に示すように、上記再生された部分を用いて、また、ＲＦＣ８２２規格の一致解析装置を用いて、データは再編成される。これにより、再生された電子メールが正しいフォーマッ

トで確実に送られる。

【００７７】

次いで、ステップＳ３１５に示すように、ＳＭＴＰプロトコルを用いて、再生された電子メールはＡＶアプリケーションにより所望の受信者に送信される。

【００７８】

しかし、ステップＳ３１１において、有用な電子メールを形成すべく電子メールの十分な部分が再生されなかったとＡＶアプリケーションが判定した場合、電子メールはステップＳ３１７において拒絶される。ステップＳ３１７では、警告テキストが所望の電子メール受信者に送られて、受信者に向けられた電子メールがシステムによって拒絶されたことを受信者に知らせる。警告テキストは、メッセージが削除された詳細な理由を含むことができる。また、警告テキストは、受信者が送信者を識別するのに役立つ情報を更に含むか、或いは電子メールが拒絶された理由を含むことができる。

【００７９】

本実施形態において使用する一致解析装置の幾つかの例を以下に詳細に説明する。これらの一致解析装置は、ステップＳ３０９において使用できる。ＲＦＣ８２２ヘッダやＭＩＭＥヘッダ或いはファイル拡張子の情報に基づいて、テキストであると表明する電子メールの構成部分は、Ｓ３０９で示すように、テキスト一致解析装置に渡される。テキスト一致解析装置は、以下に述べるように、テキストデータを構文解析し、そのテキストデータが所定の許可可能なフォーマットに一致するか否かを判定する。

【００８０】

例えば、カンマ区切り変数（ＣＳＶ：Comma Separated Variable）やリッチテキストフォーマット（ＲＴＦ）などの異なる形式のテキストファイルが幾つか存在するとき、テキスト一致解析装置は、最初に、構文解析されたデータが表明しているのはどの形式のテキストファイルであるのかを識別しなければならない。電子メールに添付されたファイルは、全て、それと関連のあるファイル拡張子を有して、ファイル形式が何であるかを示す。テキスト一致解析装置は、ＭＩＭＥヘッダ内の構文解析されたファイル拡張子を解析して、そのテキストファイルが純粋なＡＳＣＩＩファイルであるか否かを判定する。純粋なＡＳＣＩＩファイルであれば、以下に述べる通り、ＡＳＣＩＩ一致解析装置を使用すればよい。

【００８１】

一方、テキスト一致解析装置が、解析の結果、そのテキストファイルが純粋なＡＳＣＩＩ以外のファイル形式、例えばＣＳＶファイルであると判定した場合は、ＣＳＶ一致解析装置が呼び出されてＣＳＶデータを解析し、再生する。しかしながら、まず最初に、ＡＳＣＩＩ一致解析装置が、電子メール内のテキストファイルを構成しているＡＳＣＩＩ文字を解析して、そのテキスト列がＡＳＣＩＩの所定フォーマットに一致するか否かを調べ、一致していれば、そのＡＳＣＩＩファイルを再生する。

【００８２】

ＡＳＣＩＩ一致解析装置はデータを解析して、ファイルが最小のＡＳＣＩＩ所定フォーマットに一致していることを確実にする。例えば、ＡＳＣＩＩ一致解析装置は、ＡＳＣＩＩ文字３２～１２７と、４つの制御文字、すなわち、「改行」（ＬＦ＝１０）、「復帰改行」（ＣＲ＝１３）、「タブ」（ＴＡＢ＝９）および「垂直タブ」（ＶＴ＝１１）のみの再生を許可し、そしてシステムを通過することを許可する。

【００８３】

ベル文字（ＢＥＬ＝７）などの他の制御文字は、ＡＶアプリケーションによって定義されるＡＳＣＩＩファイルの所定の許可可能なフォーマット内には、存在しない。したがって、ＡＳＣＩＩ一致解析装置は、構文解析されるＡＳＣＩＩコードブロックにおいて「ＢＥＬ」文字を再生せず、そのＡＳＣＩＩ文字を拒絶する。

【００８４】

ＡＳＣＩＩ一致解析装置が実行するその他の解析例は、

・固有の行長さは１０２４文字未満であるか？

・ワード長さは２５文字未満であるか？
・文字に対するスペースの割合は所定限界以下であるか？
である。
【００８５】
データが基本所定フォーマットに一致していないために、ＡＳＣＩＩ一致解析装置がＡＳＣＩＩコードの一部分のデータを再生することができない場合はいつでも、ＡＳＣＩＩ一致解析装置は、そのデータを検査して、それが他のいずれかの形式のＡＳＣＩＩコード（例えば、ソースコード、ＢｉｎＨｅｘ、ＢＡＳＥ６４など）に一致するか否かを調べる。データが他の形式のＡＳＣＩＩコードに一致する場合、そのデータはそのＡＳＣＩＩ形式に関する一致解析装置に送られる。この一致解析装置は、上に示した例では、ソースコード一致解析装置、ＢｉｎＨｅｘ一致解析装置、或いはＢＡＳＥ６４一致解析装置である。当然のことながら、ＢＡＳＥ６４ＡＳＣＩＩコードファイルは、符号化されたデータ内に他の形式のファイルを含み得る。これらの他の形式のファイルもまた、次に、関連するファイル形式一致解析装置などに送られる。
【００８６】
上記他の形式のＡＳＣＩＩコード一致解析装置は、電子メールのこの部分のデータに対して更なる一致限定事項を有する。例えば、ファイルがチェックされて、このファイルが適切に構造化されたコードであるか否か、正しい行長を有するか否かなどが調べられる。各一致解析装置が、コンテンツおよびパラメータのデータが一致していると判定すると、すなわち、そのデータを抽出すると、抽出されたコンテンツデータは当該一致解析装置により許可所定フォーマットにて再生される。
【００８７】
ＡＳＣＩＩ一致解析装置がいったんそのタスクを終了すると、再生されたＡＳＣＩＩデータは、そのデータが表明する関連のテキスト一致解析装置に送られる。この実施形態では、テキストファイルがＣＳＶファイルである。したがって、データはＣＳＶ一致解析装置に送られる。
【００８８】
ＣＳＶ一致解析装置によって実行される検査例は以下の通りである。すなわち、ＣＳＶ一致解析装置は、パラグラフがＣＳＶファイルに対する所定フォーマットの一部でないとき、ＡＳＣＩＩデータを解析して、確実に、長いテキストパラグラフが含まれないようにする。一致しないために解析できないデータは、ＣＳＶ一致解析装置によって拒絶される。また、ＣＳＶ一致解析装置は、検査をして、例えば、デリミッター（非制限手段）の数がＣＳＶファイル内のデリミッターの通常所定数に一致するか否かを調べる。データが一致するとＣＳＶ一致解析装置が判定した場合、そのデータは同一のフォーマットに再生される。
【００８９】
このようにして、所定のフォーマットに一致するテキストファイル部分のみが、ＡＶアプリケーションの次のステージに通過できる。このテキストファイルの一致部分のみが、再生された他のデータ形式部と共に再生され、再編成されて、送信先に送られる。したがって、電子メールのウイルスを含む部分は、不一致となり、したがってブロックされ、すなわち再生されることがなく、そして好ましくは、削除される。不一致部分は、ＡＶアプリケーションを通過できなく、オペレーティングシステムに感染することが許されない。
【００９０】
一致解析装置の他の例として、ＴＩＦＦファイルを解析し再生するのに使用されるＴＩＦＦ（Tagged Image File Format）一致解析装置がある。
【００９１】
ＴＩＦＦファイルは、１組のディレクトリとタグとが所定のフォーマットで配置された構造化フォーマットを有している。イメージデータ自体が意味のある画像を表しているか否かを判定できる。しかしながら、ＴＩＦＦ一致解析装置は、イメージデータが確実に所定の限界内に収まっているかを確認するために、イメージデータを構文解析し分析する。

【００９２】
ＴＩＦＦファイル内のヘッダ情報は、正しい情報が完全で手付かずのものであるか否かを調べるために、構文解析され分析される。例えば、ＴＩＦＦ一致解析装置は、ヘッダ情報がＴＩＦＦ画像に対して妥当限界内の解像度、サイズ、被写界深度を含むものであるか否かを調べるために検査を行う。更に、ＴＩＦＦ一致解析装置は、ヘッダに示された帯片（ストリップ）の数がイメージデータと合っているか否かを判定する。
【００９３】
ＴＩＦＦファイルは、典型的には、ＬＺＷ（Lempel-Ziv-Welch）圧縮技術を通常使用して圧縮される。帯片の長が妥当な所定限界内にあるか否かを調べるために、各ＴＩＦＦ帯片は一致解析装置によって解凍される。例えば、帯片長が最大イメージサイズの限界以下の場合（例えば、標準のＡ０用紙サイズより大きい場合）、帯片は拒絶される。ＴＩＦＦ一致解析装置が１つの帯片を拒絶すると、ＴＩＦＦファイル全体が拒絶される。
【００９４】
また、ＴＩＦＦ一致解析装置は、ＴＩＦＦファイル内のタグ（すなわち、パラメータデータ）に関する解析を実行する。タグは所定の許可フォーマットに照らして検査されて、例えば、タグが（ヘッダにおけるタグ情報のディレクトリに従って）指定された順序にあるか否か、タグが互いに正しく関連づけられているか否かについて調べられる。
【００９５】
ＴＩＦＦ一致解析装置が、データが所定の許可フォーマットに一致すると判定すると、データが再生されて、オリジナルのファイル名を有する再生ＴＩＦＦファイルが作成される（上記ファイル名は所定のフォーマットに一致する）。再生ＴＩＦＦファイルは電子メールサーバに送られて電子メールに再編成される。
【００９６】
ＴＩＦＦファイル自体の中に他のイメージ形式をもたせることも可能である。例えば、ＪＰＥＧ画像をＴＩＦＦファイル内にカプセル化してもよい。ＴＩＦＦ一致解析装置によって異なるイメージ形式が検出された場合、そのイメージに関連するデータが別の一致解析装置、この例では、ＪＰＥＧ一致解析装置に送られる。次いで、ＪＰＥＧ一致解析装置は、そのデータを構文解析し分析して、データが予期されるＪＰＥＧフォーマットに一致するか否かを調べる。一致している場合、そのデータをＪＰＥＧフォーマットで再生する。再生されたデータは、次に、再生されたＴＩＦＦファイル内に再編成される。上記ＴＩＦＦファイルは、その後、更に再生電子メールを再編成するために使用される。次に、この電子メールは電子メールサーバに渡される。
【００９７】
本実施形態における別の利用可能な選択肢は、ＡＶアプリケーションが、電子メールの不一致箇所に代えて、警告テキストを挿入することである。すなわち、電子メールの再生時に、一致解析装置が不一致箇所のデータを構文解析して、その箇所の一部が所定の許可可能なフォーマットに一致しないと判定された場合、一致解析装置は、不一致部分の代わりに、警告テキストを挿入して、その電子メールの一部がＡＶアプリケーションによって拒絶されたことを相手の電子メール受信者に知らせる。或いは、不一致のために一致解析装置が電子メールの一部分全体をブロックする場合、ＡＶアプリケーションは、警告テキストを電子メール内に挿入して、電子メールの一部分がブロックされたことを相手の受信者に知らせる。すなわち、電子メールの一部分が、再生されなかったこと、更に好ましくは消去されたことを相手の受信者に知らせる。
【００９８】
第３実施形態
次に、本発明の第３実施形態を、図５を参照して説明する。
【００９９】
この第３実施形態は、第２実施形態の全ての特徴が組み込まれ、第２実施形態と関連して述べた選択肢（オプション）のいずれをも含むものである。
【０１００】

図５は、本第３実施形態によるプロセスのフローチャートを示す。

【０１０１】

本実施形態は、ＡＶアプリケーションが電子メールの一部、部分または全体（本実施形態では「不一致部分」という）をブロックする状況に関する。ステップＳ５０１において、部分が不一致であるか否かについて、したがって、部分がブロックされるべきか否かについて、ＡＶアプリケーションが判定を行う。ＡＶアプリケーションによってブロックされた場合、その不一致部分は脅威フィルタアプリケーションに送られて、ステップＳ５０３に示すように、その不一致部分が脅威であるか否かを確認する。

【０１０２】

脅威フィルタアプリケーションは、システムユーザの選択に基づいて、その不一致部分が真の脅威と見なされるか否かを判定する。上記システムは、そのメモリ内に、脅威と考えられないファイル形式のリストと、これらファイル形式に付随したソースとを格納している。したがって、システムは、ファイルの送信者とファイル形式に基づいて、そのファイルが通過許可されるか否かを判定することができる。

【０１０３】

ステップＳ５０３での判定において、ファイル形式が、関連するソースから、許可可能としてリストアップされたものの一つではないと判定された場合、そのファイルはステップＳ５０５でブロックされる。

【０１０４】

ファイル形式が許可可能と見なされた場合、ステップＳ５０７において、不一致部分はＡＶアプリケーションを迂回する。ＡＶアプリケーションは、ステップＳ５０９において、受信ファイルの残りを再生する。そして、ＡＶアプリケーションは、ステップＳ５１１において、ファイルの再生された一致部分と迂回した不一致部分とを再編成する。

【０１０５】

例えば、バンキングシステムが多数の電子メールを既知の送信者から受信し、その多数の電子メールが複雑なマクロを組み込んだスプレッドシートを含んでいる場合、これらのマクロが、スプレッドシートの添付ファイル内のマクロ用所定許可フォーマットに収まらないことがある。その場合、マクロ一致解析装置は電子メールのこの部分をブロックすることになる。

【０１０６】

しかしながら、誰がその電子メールを送っているかをバンキングシステムが判定でき、また、送信者が、バンキングシステムの信頼できる相手として、これらのファイル形式のデータベース内に入力されているときは、電子メールの中のスプレッドシートは脅威とは見なされない。したがって、システムユーザは上記脅威フィルタアプリケーションをセットアップして、これら不一致マクロ部分が、ＡＶアプリケーションを迂回し、且つ、電子メールの再生された部分と共に再編成された電子メールとすることができる。

【０１０７】

これに代替わる方法として、脅威フィルタアプリケーションは或るモードで動作させることができる。これによって、ＡＶアプリケーションから受け取った再生ファイルが、送信先のシステムに連通することを許可されるべきか否かを判定する。不一致部分自体は即座にファイル全体が拒絶される程にはＡＶアプリケーションに対して不一致ではないが、結果的にはオリジナルのファイルと実質的に異なる再生一致ファイルとなる、そのような不一致部分を含むファイルをＡＶアプリケーションが受け取った場合、再生ファイルは脅威フィルタアプリケーションに送られる。例えば、オリジナルのファイルサイズは、ＡＶアプリケーションによって再生されないマクロ内の膨大な数の書直し言語に起因して、再生された一致ファイルのサイズよりもかなり大きなものになり得る。

【０１０８】

脅威フィルタアプリケーションは、ファイル形式がそのファイルに対して承認されたソースから送られているか否かを判定する。送られている場合は、脅威フィルタアプリケーションは、そのファイル形式がシステムを通過することを許可する。

【０１０９】
他の実施形態
本発明の実施形態は、単なる例証としてここに記載されているに過ぎないこと、また、本発明の範囲から逸脱することなく種々の変更および変形がなし得ることが理解される。
【０１１０】
本発明は、電子ファイルをソースから送信先に移す如何なるシステムにおいても、実施し得ることが理解される。本発明の目的とする電子ファイル送信方法は、特定の方法に限定されるものではない。すなわち、例えば、一つのコンピュータシステムのハードウェア内の１つの構成要素から他の構成要素に、電子ファイルを転送してもよい。或いは、例えば、基地局から空中インタフェースを介して移動電話装置に、電子ファイルを転送してもよい。また、例えば、ローカルエリアネットワーク（ＬＡＮ）や広域ネットワーク（ＷＡＮ）を介して、或いはインターネットを経由して、電子ファイルを伝送してもよい。
【０１１１】
更に、上述した実施形態の更なる選択肢として、ユーザのためにオーバーライド装置を備えて、電子ファイル受領時に、ユーザが、ＡＶアプリケーションまたは脅威フィルタアプリケーションによってなされた判定を手動でオーバーライド（処置）することが考えられる。すなわち、不一致に起因してＡＶアプリケーション内の一致解析装置が電子メールの一部または部分または全体をブロックするときであっても、電子メールの不一致なものの再生、再編成を許可する選択肢がユーザに与えられる。
【０１１２】
この選択肢の実施の一例は、相手の受信者にテキスト警告書を提供して、不一致と解析された電子メールは、所定の許可フォーマットに一致するものと同様にシステム通過を許可すべきであるか否かを受信者に尋ねることである。この警告に対する応答により、可能であれば、電子メールを再生し、再編成する命令が一致解析装置に与えられる。或いはそれに代わって、オリジナルの電子メールは、ＡＶアプリケーションおよび脅威フィルタアプリケーションの両方を迂回することが許可されて、再生されることなくシステムを通過する。
【０１１３】
更に、第２実施形態で説明したＡＶアプリケーションは、ＩＳＰ電子メールサーバ以外の場所に設置し得ることが考えられる。例えば、ＡＶアプリケーションは、受信者の電子メールクライアントサーバに配置し設置してもよい。こうして、電子メールクライアントサーバによってハードディスクドライブ上の受信者受信ボックスに送られた電子メールが、上述した再生電子メールとなる。
【０１１４】
更に、ＡＶアプリケーションは、限定的なものではないが、シリコン、ガリウム砒素（ＧａＡｓ）、リン化インジウム（ＩｎＰ）などの半導体素子において、ハードワイヤ接続してもよいことが考えられる。すなわち、ＡＶアプリケーションは定量化可能なタスクを有している。この定量化可能なタスクは、所定の一致フォーマットを形成するプロセスに対して更新する必要がない。構文解析、分析、再生および再編成を含むＡＶアプリケーションのタスクを実行するのに必要な命令は、任意の適切な半導体装置において、実現可能である。また、ＡＶアプリケーションを実行するのに必要な命令は、半固定メモリ素子や固定メモリ素子に格納しておくことが可能である。そのとき、上記メモリ素子は、接続されたプロセッサと協働して作動し、ＡＶアプリケーションを実行する。これらの場合、本発明を、保護すべきコンピュータとは分離して、別個の装置として提供することが可能となる。上記別個の装置（例えば、モデムカード、ネットワークアダプタカード、またはディスクドライブコントローラなどのカード）には、保護すべきコンピュータとは別のプロセッサやメモリハードウェアが含まれる。そうすることによって、到来する電子ファイルを保護すべきコンピュータのファイルシステムその他のリソースから完全に隔離し、通常書込みや更新のできない場所に上記電子ファイルを保存して、それによりＡＶアプリケーション自体に対する“トラップドア”攻撃を回避するという利点が得られる。すなわち、

一定レベルの物理的セキュリティが得られるという利点がある。上記半導体装置はプロセッサとメモリ素子とから成り、上記プロセッサはメモリ素子からのＡＶアプリケーションを実行させ、到来ファイルを隔離するために、上記ファイルをメモリ素子に保存する。

【０１１５】

更に、上記半導体装置は、従来法を用いる適当なネットワークカードの一部として設けることが考えられる。このようにして、ネットワークカードは、上記方法を用いて受信電子ファイルを再生することによって、ネットワークを不適切なコードおよびデータから確実に保護する手段として、通信ネットワーク内で用いることができる。

【０１１６】

更に、上記第１実施形態で説明した電子ファイルは、コンピュータ装置によって受け取られ、着脱可能なメモリ素子に保存することが考えられる。例えば、電子ファイルは、直接またはワイヤレスの媒体を介して、コンピュータ装置に接続されたＵＳＢディスク装置、スマートカード、セキュアデジタル（ＳＤ）メモリ装置、マルチメディアカード（ＭＭＣ）メモリ装置、コンパクトフラッシュ（ＣＦ）カード１型または２型、スマートメディア（ＳＭ）カード、ＸＤカード、フロッピーディスク、ＺＩＰドライブ、ポータブルハードドライブ、その他の適切なメモリ装置に保存することができる。

【０１１７】

更に、本出願で説明されるオペレーティングシステムは、ファイルを使用するあらゆるシステムであり得ると考えられる。例えば、埋込み型システム、ルータ、ネットワークカード等である。

【０１１８】

更に、他のスクランブル方法を用いて、確実に、受信された実行可能ファイルが自動的には実行され得ないことが考えられる。例えば、スクランブル方法は、バイトスワップ法を用いて、受信バイトの各ペアを格納する。この例では、ＡＢＣＤＥＦの６バイトがＡＶアプリケーションによって受信された場合であって、バイトＡが最初にバイトＦが最後に受信された場合には、上記ＡＢＣＤＥＦはＢＡＤＣＦＥの順でメモリに格納される。最初のバイトＡは２番目のメモリ位置に格納され、２番目のバイトＢは最初のメモリ位置に格納される。この反転は、後続のメモリ位置における受信バイトの各ペアに対しても、生じる。このようにして、如何なる実行可能なコードも自動的に動作することができないので、如何なる感染電子ファイルも、ＡＶアプリケーションや送信先のオペレーティングシステムに感染することができない。

【０１１９】

誤解を避けるために述べておくと、本明細書によって、上述の新規実施形態のいずれか或いは全てに対して、単独で或いは組み合わせで、保護が求められている。

【０１２０】

本発明の様々な局面および実施形態およびそれらの変形例について説明したので、本発明が、その原理から逸脱することなく、構成や詳細において変更され得ることを当業者は認識する。我々は、全ての実施形態および請求項の精神と範囲に含まれる変更や変形について権利を主張する。

【図面の簡単な説明】

【０１２１】

【図１Ａ】本発明の一実施形態による電子ファイルシステムのブロックダイアグラムを示す。

【図１Ｂ】本発明の実施形態での使用に適したコンピュータシステムを示す。

【図１Ｃ】本発明の一実施形態によるプロセスのフローチャートを示す。

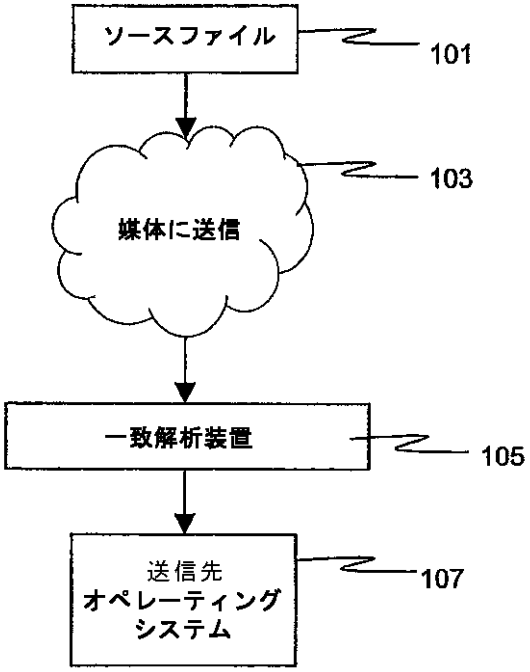
【図２】本発明の第２実施形態による電子メールシステムのブロックダイアグラムを示す。

【図３】本発明の第２実施形態によるプロセスのフローチャートを示す。

【図４】電子メールを形成する異なる部分のレイアウト例を示す。

【図５】本発明の第３実施形態によるプロセスのフローチャートを示す。

【図１Ａ】



【図１Ｂ】

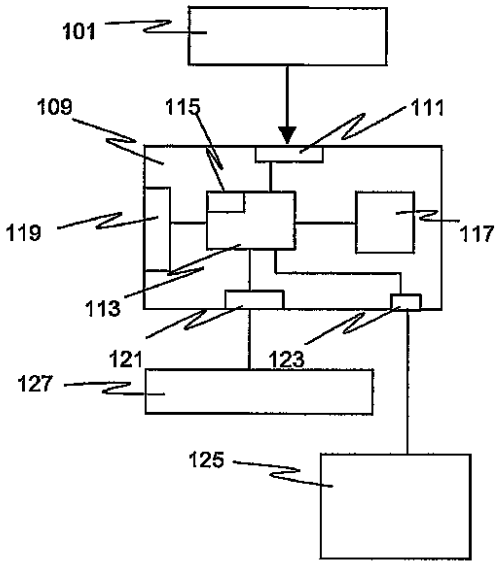
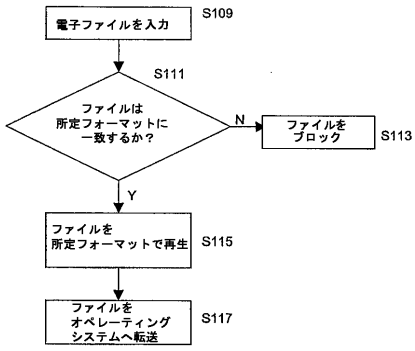


FIG. 1B

【図１Ｃ】



【図２】

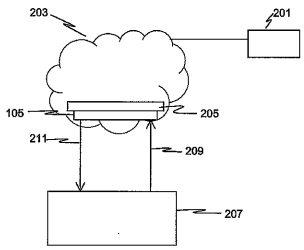
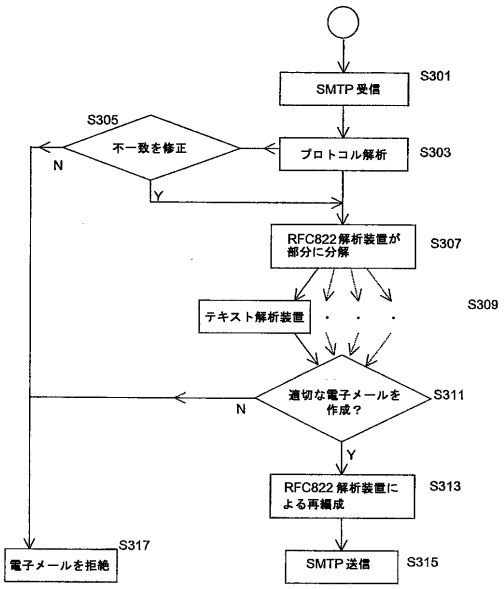
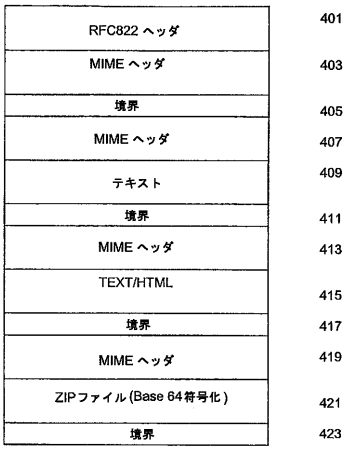


FIG. 2

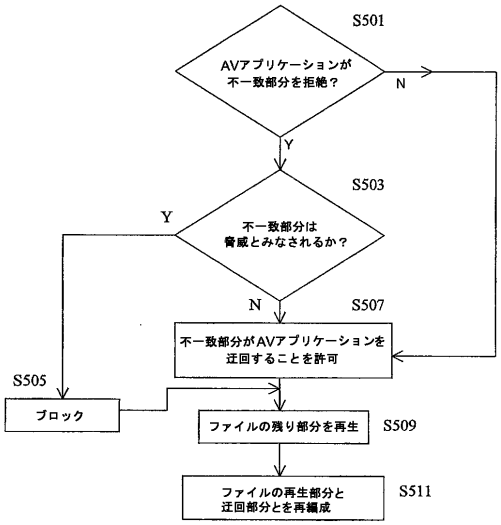
【図３】



【図４】


RFC822 ヘッダ
401
MIME ヘッダ
403
境界
405
MIME ヘッダ
407
テキスト
409
境界
411
MIME ヘッダ
413
TEXT/HTML
415
境界
417
MIME ヘッダ
419
ZIPファイル (Base 64符号化)
421
境界
423

【図５】


S501
AVアプリケーションが
不一致部分を拒絶?
N
Y
S503
不一致部分は
脅威とみなされるか?
Y
N
S507
不一致部分がAVアプリケーションを
迂回することを許可
S505
ブロック
ファイルの残り部分を再生
S509
ファイルの再生部分と
迂回部分とを再編成
S511

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002107

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/196104 A1 (BABER STEPHEN C ET AL) 16 October 2003 (2003-10-16) page 1, paragraph 10 - page 2, paragraph 14 page 2, paragraph 20 - page 3, paragraph 35 claims 7,10,11	1-25
X	US 2003/145213 A1 (CARBONE KEVIN J) 31 July 2003 (2003-07-31) page 2, paragraph 22 - page 3, paragraph 34	1,18,19, 22-24

-/--

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 September 2006	04/10/2006

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Arbutina, Ljiljana

2

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/GB2006/002107

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2003/079158 A1 (TOWER JAMES BRIAN ET AL) 24 April 2003 (2003-04-24) page 3, paragraph 44 page 5, paragraphs 89,90 page 7, paragraph 99 page 7, paragraph 103 - page 8, paragraph 108 figures 6,7,9,16	1,18,19, 22-24
X	US 2004/199594 A1 (RADATTI PETER V ET AL) 7 October 2004 (2004-10-07) page 1, paragraph 17 page 3, paragraphs 33,34,37 page 4, paragraph 55 - paragraph 58	23,24
X	"MailStreet Features and Benefits" 21 April 2004 (2004-04-21), , XP002356823 Retrieved from the Internet: URL:http://web.archive.org/web/20040421044456/http://www.mailstreet.com/defender/features.asp> [retrieved on 2005-11-13]	23,24
A	the whole document	11,12
X	"Checking of incoming files for macro viruses" ONLINE, [Online] 2004, XP002376936 Retrieved from the Internet: URL:http://www.bsi.de/english/gshb/manual/s/s04044.html> [retrieved on 2006-11-04] the whole document	23,24
A	US 6 401 210 B1 (TEMPLETON RANDALL F) 4 June 2002 (2002-06-04) column 1, line 65 - column 2, line 4	7-9

2

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/GB2006/002107

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2003196104 A1	16-10-2003	NONE	
US 2003145213 A1	31-07-2003	NONE	
US 2003079158 A1	24-04-2003	WO 03036480 A2	01-05-2003
US 2004199594 A1	07-10-2004	US 2004199773 A1 US 2002198945 A1	07-10-2004 26-12-2002
US 6401210 B1	04-06-2002	NONE	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,LY,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．コンパクトフラッシュ
２．フロッピー

(72)発明者 ニコラス・ジョン・スケイルズ
英国シーエム３・２キューワイ、エセックス、ターリング、スパローズ・ファーム・ロード、スパローズ・ファーム

Ｆターム(参考) 5B276 FD08