(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2007-508608
(P2007-508608A)
(43)公表日　平成19年4月5日(2007.4.5)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 13/00 (2006.01)	G06F 13/00 610Q	

審査請求 未請求　予備審査請求 未請求　（全 19 頁）

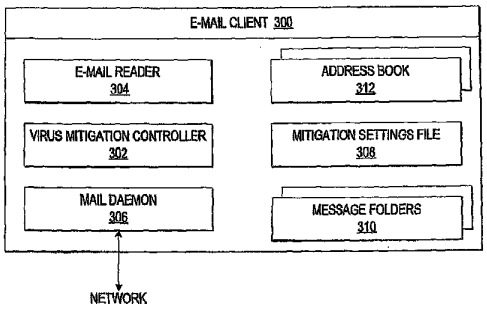
(21)出願番号	特願2006-530243 (P2006-530243)
(86)(22)出願日	平成16年9月13日 (2004.9.13)
(85)翻訳文提出日	平成18年6月6日 (2006.6.6)
(86)国際出願番号	PCT/EP2004/052153
(87)国際公開番号	WO2005/039138
(87)国際公開日	平成17年4月28日 (2005.4.28)
(31)優先権主張番号	10/682,421
(32)優先日	平成15年10月9日 (2003.10.9)
(33)優先権主張国	米国 (US)

(71)出願人　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)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】自己増殖型Ｅメール・ウイルスの軽減

(57)【要約】
【課題】　自己増殖型Ｅメール・ウイルスを軽減するための方法、システムおよびプログラムを提供する。
【解決手段】　添付ファイル付き電子メール・メッセージを、受信対象者に送信する旨の要求を受信する。前記受信対象者の特性値を、前記添付ファイルの最大受信者許容値と比較する。前期受信対象者の前記特性値が、前記添付ファイルの前記最大受信者許容値を超える場合には、前記電子メール・メッセージを送信する前に、送信者認証が必要になる。前記送信者認証は、ウイルスが前記電子メール・メッセージの送信によって自己増殖しようとしている場合には、前記試みを軽減するようなものであることが必要である。
【選択図】　図３



【特許請求の範囲】
【請求項１】
添付ファイル付き電子メール・メッセージを、少なくとも１人の受信対象者へ送信する旨の要求を受信し、
前記少なくとも１人の受信対象者の特性値を、前記添付ファイルの最大受信者許容値と比較し、
前記少なくとも１人の受信対象者の前記特性値が、前記添付ファイルの前記最大受信者許容値を超えるのに応答して、前記電子メール・メッセージを送信する前に送信者認証を要求して、ウイルスが前記電子メール・メッセージを送信することによって自己増殖しようとしている場合に、前記送信を軽減すること
を含む、自己増殖型電子メール・ウイルスを軽減する方法。
【請求項２】
前記少なくとも１人の受信対象者の前記特性値を、前記電子メール・メッセージの最大受信者許容値と比較し、
前記少なくとも１人の受信対象者の前記特性値が前記電子メール・メッセージの受信者の前記最大受信者許容値を超えるのに応答して、前記電子メール・メッセージを送信する前に送信者認証を要求すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項３】
添付ファイル付き電子メール・メッセージを送信する旨の要求の受信が、前記電子メール・メッセージ内に添付ファイルとして組み込まれたファイルを検出すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項４】
前記少なくとも１人の受信対象者の前記特性値と、最大受信者許容値との比較が、
前記少なくとも１人の受信対象者の少なくとも１つのアドレスを、受信者のアドレス帳と比較し、
前記少なくとも１人の受信対象者の前記少なくとも１つのアドレスのうち、受信者の前記アドレス帳のアドレスにマッチするアドレスの数を計算し、
前記マッチするアドレスの数が、受信者の前記アドレス帳内のアドレスの最大許容値を超えているか否かを確定すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項５】
前記少なくとも１人の受信対象者の前記特性値と、最大受信者許容値との比較が、
前記少なくとも１人の受信対象者の数を、或る種の前記添付ファイルの最大受信者許容値と比較すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項６】
前記電子メール・メッセージを送信する前の送信者認証の要求が、
認証としてのパスワードの入力と送信者による手入力のうち、少なくとも１つを要求すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項７】
ネットワーク管理者およびユーザのうち、少なくとも一方から前記最大受信者許容値を受信すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項８】
前記送信者認証の拒絶の受信に応答して、前記電子メール・メッセージが阻止された旨をネットワーク管理者に通報すること
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１に記載の方法。
【請求項９】

ネットワークに通信可能に接続されたコンピューティング・システム
を含み、
前記コンピューティング・システムは、
添付ファイル付き電子メール・メッセージを少なくとも１人の受信対象者に送信するための要求を受信する手段と、
前記少なくとも１人の受信対象者の特性値を、前記添付ファイルの最大受信者許容値と比較する手段と、
前記少なくとも１人の受信対象者の前記特性値が前記添付ファイルの前記最大受信者許容値を超えるのに応答して、前記電子メール・メッセージを送信する前に送信者認証を要求する手段と
をさらに含む、自己増殖型電子メール・ウイルスを軽減するシステム。
【請求項１０】
前記コンピューティング・システムは、
前記少なくとも１人の受信対象者の前記特性値を、前記電子メール・メッセージの最大受信者許容値と比較する手段と、
前記少なくとも１人の受信対象者の前記特性値が前記電子メール・メッセージの受信者の前記最大受信者許容値を超えているのに応答して、前記電子メール・メッセージを送信する前に送信者認証を要求する手段と
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１１】
添付ファイル付き電子メール・メッセージを送信する旨の要求を受信する前記手段は、前記電子メール・メッセージ内に添付ファイルとして組み込まれたファイルを検出する手段
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１２】
前記少なくとも１人の受信対象者の前記特性値を最大受信者許容値と比較する手段は、
前記少なくとも１人の受信対象者の少なくとも１つのアドレスを、受信者のアドレス帳と比較する手段と、
受信者の前記アドレス帳のアドレスとマッチする、前記少なくとも１人の受信対象者の前記少なくとも１つのアドレスの数を計算する手段と、
前記マッチするアドレスの数が、受信者の前記アドレス帳内のアドレスの最大許容値を超えているか否かを確定する手段と
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１３】
前記少なくとも１人の受信対象者の前記特性値を最大受信者許容値と比較する手段は、
前記少なくとも１人の受信対象者の数を、或る種の前記添付ファイルの最大受信者許容値と比較する手段
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１４】
前記電子メール・メッセージを送信する前に、送信者認証を要求する前記手段は、
認証としてのパスワードの入力と送信者の手入力のうち、少なくとも１つを要求する手段
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１５】
ネットワーク管理者とユーザのうち少なくとも一方から、前記最大受信者許容値を受信する手段

をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１６】
前記送信者認証の拒否の受信に応答して、前記電子メール・メッセージが阻止された旨をネットワーク管理者に通報する手段
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項９に記載のシステム。
【請求項１７】
自己増殖型電子メール・ウイルスを軽減するためのプログラムであって、該プログラムがコンピュータに、
添付ファイル付き電子メール・メッセージを少なくとも１人の受信対象者へ送信する旨の要求を受信する機能と、
前記少なくとも１人の受信対象者の特性値を、前記添付ファイルの最大受信者許容値と比較する機能と、
前記少なくとも１人の受信対象者の前記特性値が前記添付ファイルの前記最大受信者許容値を超えているのに応答して、前記電子メール・メッセージを送信する前に、送信者認証を要求する機能と
を実現させるプログラム。
【請求項１８】
前記少なくとも１人の受信対象者の前記特性値を、前記電子メール・メッセージの最大受信者許容値と比較する機能と、
前記少なくとも１人の受信対象者の前記特性値が前記電子メール・メッセージの受信者の前記最大受信者許容値を超えるのに応答して、前記電子メール・メッセージを送信する前に、送信者認証を要求する機能と
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【請求項１９】
添付ファイル付き電子メール・メッセージの送信要求を受信する前記機能は、
前記電子メール・メッセージ内に添付ファイルとして組み込まれているファイルを検出する機能
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【請求項２０】
前記少なくとも１人の受信対象者の前記特性値を、最大受信者許容値と比較する前記機能は、
前記少なくとも１人の受信対象者の少なくとも１つのアドレスを、受信者のアドレス帳と比較する機能と、
受信者の前記アドレス帳のアドレスとマッチする、前記少なくとも１人の受信対象者の前記少なくとも１つのアドレスの数を計算する機能と、
前記マッチするアドレスの数が受信者の前記アドレス帳でアドレスの最大許容値を超えているか否かを確定する機能と
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【請求項２１】
前記少なくとも１人の受信対象者を、最大受信者許容値と比較する機能は、
前記少なくとも１人の受信対象者を、或る種の前記添付ファイルの最大受信者許容値と比較する機能
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【請求項２２】

前記電子メール・メッセージを送信する前に、送信者認証を要求する機能は、
認証としてのパスワードの入力と送信者の手入力のうち少なくとも１つを要求する機能
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【請求項２３】
ネットワーク管理者とユーザのうち少なくとも一方から前記最大受信者許容値を受信する機能
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【請求項２４】
前記送信者認証の拒否に応答して、前記電子メール・メッセージが阻止された旨をネットワーク管理者に通報する機能
をさらに含む、自己増殖型電子メール・ウイルスを軽減する、請求項１７に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に、改良型電子メールシステムに関し、特に、本発明は、自己増殖型電子メール・ウイルスを軽減することに関する。さらに具体的には、本発明は、受信対象者の数が１ユーザ当たり受信者の最大許容値を超える場合には、添付ファイルを含む電子メールの送信に対して追加認証を与えるよう送信者に要求することによって、自己増殖型電子メール・ウイルスを軽減することに関する。これらのウイルスは、感染者がＥメール・メッセージを生成し、これを前記感染者のアドレス帳の各Ｅメール・アドレス宛に送信することによって自己増殖することを目的としている。特定の企業が使用しているネットワーク内では、各従業員のＥメール・アドレス帳に、他の全ての従業員のＥメール・アドレスが含まれていることが普通である。自己増殖型Ｅメール・ウイルスは、このようなシステムの中で、従業員の１人に到達すると、急速かつ広範囲に拡散することができる。自己増殖型Ｅメール・ウイルスのもう一つの機能は、添付ファイル付き電子メールのファイルを添付するか、または組み込むことである。
【背景技術】
【０００２】
「コンピュータ・ウイルス」は、コンピュータのコンピュータ・ファイルおよび他の機密領域に侵入するように作られたプログラムである。多くの場合、ウイルスの目的は、前記コンピュータのセキュリティを脅かすことである。例えば、ウイルスは、前記コンピュータに保存されたデータまたは、前記コンピュータにアクセスできるネットワーク・ファイル・サーバに保存されたデータを消去したり、破壊したりすることができる。別の例をあげると、ウイルスは、前記コンピュータ・ユーザの許可なく、機密情報を取得して転送することができる。
【０００３】
コンピュータ・ユーザがウイルス感染ファイルを電子メール（Ｅメール）で他のコンピュータ・ユーザに送信した場合、ウイルスが拡散することが多いが、ウイルスは、ウイルス感染ファイルがネットワークを経由して１つのコンピュータから他のコンピュータにコピーされた場合にも、拡散する可能性がある。ある種のＥメール・ウイルスの中には、ウイルス感染したコンピュータ・システム側の介入が、ほとんどまたは全くないまま、コンピュータからコンピュータへ拡散し、無許可配信によってシステム上に保存されたファイルのセキュリティを破壊することのできるものがある。さらに、前記Ｅメール・ウイルスは、しばしば自分自身をファイルに添付させ、前記ファイルを開いたコンピュータに感染することがある。
【０００４】
コンピュータ・ウイルスを防御する標準的な方法は、ウイルス・スキャナーを用いて、

コンピュータやネットワーク上のウイルスの存在を検出することである。ウイルス・スキャナーにより、かなりの防御ができるが、ほとんどのウイルス・スキャナーは、恒常的な更新を必要としており、前記更新ができるまでは、ウイルス・スキャナーは新しいウイルスを見つけることができない場合がある。そのため、周知のウイルスを探すウイルス・スキャナーに加えて、複数のセキュリティ層を生成すると好都合である。

【０００５】

前記複数のセキュリティ層内で、自己増殖型Ｅメール・ウイルスの拡散を阻止する方法を見つける必要がある。自己増殖型Ｅメール・ウイルスは、ウイルス感染Ｅメールを複数の受信者に送信することが多いため、最大数を超える受信者がＥメールを受信するよう選定されている場合を検出することによって、ウイルスの増殖を阻止する必要がある。具体的には、このような自己増殖型Ｅメール・ウイルスは、自分自身を添付ファイル内に組み込んだり、配信対象ではないファイルを添付したりすることが多いため、送信者からの添付ファイルまたはファイルのコピーを含むＥメールの最大受信者数を、特定する必要がある。そのため、Ｅメールを送信する前にスキャニングし、添付ファイル付き前記Ｅメールが、添付ファイル付きＥメール別アドレスのセット許容値以上の受信者宛である場合、送信者の追加認証を必要とする方法、システムおよびプログラムを準備しておくと好都合であろう。

【発明の開示】

【発明が解決しようとする課題】

【０００６】

それ故に、上記を考慮して、本発明の目的は、改良型Ｅメールシステムを提供することである。

【０００７】

本発明のもう一つの目的は、Ｅメール・ウイルスの増殖を軽減する方法、システムおよびプログラムを提供することである。

【０００８】

本発明のさらにもう一つの目的は、受信対象者の数が、添付ファイル付きＥメールに関わる受信者の最大許容値を超える場合、添付ファイルを含むＥメールの送信に関して、追加認証を提供するよう送信者に要求することによって、Ｅメール・ウイルスの増殖を軽減する方法、システムおよびプログラムを提供することである。

【課題を解決するための手段】

【０００９】

本発明の一側面に従って、添付ファイル付き電子メール・メッセージを受信対象者に送信する旨の要求が、受信される。前記受信対象者の特性値を、前記添付ファイルの最大受信者許容値と比較する。前記受信対象者に関する前記特性値が、前記添付ファイルの前記最大受信者許容値を超える場合には、前記電子メール・メッセージを送信する前に、送信者認証が必要になる。前記送信者認証は、ウイルスが前記電子メール・メッセージを送信することによって自己増殖しようとしている場合に、前記試みを軽減するために必要となるものである。

【００１０】

さらに、前記受信対象者の特性値を、単一の電子メール・メッセージの最大受信者許容値と比較する。その後、前記受信対象者の前記特性値が、前記単一の電子メール・メッセージの最大受信者許容値を超える場合にも、前記電子メール・メッセージを送信する前に、送信者認証が求められる。

【００１１】

前記最大受信者許容値は、ファイル毎に特定してもよいし、全てのファイルについて特定してもよい。最大受信者許容値は、前記アドレス帳のアドレスの比率、または前記アドレス帳の特定カテゴリ内のアドレス比率によって、特定される。さらに、最大受信者許容値は、一定の数値限定でもよい。前記最大受信者許容値は、受信対象者、前記選定された受信対象者、または、前記アドレス帳にも含まれている受信対象者の総人数に基づく。前

記受信対象者の特性値は、前記最大受信者許容値によって特定された数値の種類に基づいて、確定される。

【００１２】

本発明の一側面によれば、前記送信者認証は、前記送信する電子メール・メッセージを認証するパスワードを入力するよう、前記送信者に求める要求である。あるいは、前記送信者認証は、前記送信する電子メール・メッセージを認証するある種の手入力を入力するよう、前記送信者に求める要求である。

【００１３】

本発明のもう一つの側面によれば、送信者が前記送信する電子メール・メッセージを認証しない場合、前記電子メール・メッセージは阻止される。さらに、送信者が電子メール・メッセージの送信を阻害する場合、前記ネットワーク管理者または他のシステム監視機関に警報を送信することが好ましい。

【００１４】

本発明の全ての目的、特徴および利点は、以下の詳細に記述された説明で、明らかとなる。

【発明を実施するための最良の形態】

【００１５】

さて、図面、特に図１を参照すると、本方法、システムおよびプログラムが実施されるコンピュータ・システムの一実施形態が表記されている。本発明は、様々なコンピューティング・システムや多数の異なるオペレーティング・システム下の電子装置を含む、様々なシステムにおいて、実施できる可能性がある。

一般的に、本発明は、コンピュータ・システム、即ち前記コンピュータ・システムにアクセス可能な記憶装置内のデータを操作するようなコンピュータ業務を行うシステムにおいて、実施されている。さらに、前記コンピュータ・システムは、少なくとも１つの出力デバイスおよび少なくとも１つの入力デバイスを含んでいる。

【００１６】

一実施形態において、コンピュータ・システム１０は、コンピュータ・システム１０の中の、情報を通信するバス２２または他の通信デバイスと、情報を処理するためにバス２２に結合されているプロセッサ１２などの処理デバイスの少なくとも１つとを含む。バス２２は望ましくは、ブリッジとアダプタとによって接続されコンピュータ・システム１０の中で複数のバス・コントローラに制御される低待ち時間パスと高待ち時間パスを含んでいる。コンピュータ・システム１０は、サーバ・システムとして実施される場合、一般的には、ネットワーク・サービス処理能力を向上させることを目的とした複数のプロセッサを含む。

【００１７】

プロセッサ１２は、ＩＢＭのＰｏｗｅｒＰＣ^{TM}プロセッサなどの汎用プロセッサであればよく、それは通常動作中、ランダム・アクセス・メモリ（ＲＡＭ）１４などの動的記憶装置およびリード・オンリー・メモリ（ＲＯＭ）１６などの静的記憶装置からアクセスできるオペレーティング・システムおよびアプリケーション・ソフトウェアに制御されて、データを処理する。前記オペレーティング・システムは望ましくは、グラフィカル・ユーザ・インターフェース（ＧＵＩ）を前記ユーザに提供する。好適な実施形態において、アプリケーション・ソフトウェアは、プロセッサ１２で実行される場合、図９のフローチャートに表記されている動作および本明細書に記述されている他の動作を実行する、機械で実行可能な指令を含む。あるいは、本発明の前記ステップは、前記ステップを行うための配線論理を含む特定のハードウェア・コンポーネントによって、あるいは、プログラムされたコンピュータ・コンポーネントおよびカスタム・ハードウェア・コンポーネントの任意の組み合わせなどによって、行ってもよい。

【００１８】

本発明は、本発明によるプロセスを実施するためにプログラム・コンピュータ・システム１０に用いられる、前記機械で実行可能な指令を保存している機械読取り可能な媒体に

含まれるコンピュータ・プログラムとして提供してもよい。ここで用いられている「機械読取り可能な媒体」という用語は、コンピュータ・システム１０のプロセッサ１２または他のコンポーネントに対する実行指令の提供に関与する任意の媒体を含む。

このような媒体は、不揮発性媒体、揮発性媒体および送信媒体など、必ずしもそれらに限定されないが、それらを含む多くの形態をとってもよい。不揮発性媒体の一般的な形態を挙げると、例えば、フロッピー・ディスク、フレキシブル・ディスク、ハード・ディスク、磁気テープまたは任意の他の磁気媒体、コンパクト・ディスクＲＯＭ（ＣＤ－ＲＯＭ）または任意の他の光媒体、パンチ・カードまたは任意の他の穴パターン付き物理的媒体、プログラム可能ＲＯＭ（ＰＲＯＭ）、消去可能ＰＲＯＭ（ＥＰＲＯＭ）、電気的ＥＰＲＯＭ（ＥＥＰＲＯＭ）、フラッシュ・メモリ、任意の他のメモリ・チップまたはカートリッジ、あるいはコンピュータ・システム１０から読み出すことができ指令を保存するのに適した任意の他の媒体などがある。本実施形態において、不揮発性媒体の一例は、コンピュータ・システム１０の内部コンポーネントと記述されている大容量記憶デバイス１８であるが、それは外部デバイスによっても提供されることがわかるであろう。揮発性媒体は、ＲＡＭ１４などの動的メモリを含む。送信媒体は、バス２２を構成する同軸ケーブル、銅線或いは光ファイバーを含む。送信媒体はまた、高周波または赤外線データ通信中に生成される音波または光波の形態をとることもできる。

【００１９】

さらに、本発明は、コンピュータ・プログラムとしてダウンロードすることもできるが、前記プログラムの指令は、サーバ４０などのリモート・コンピュータから、バス２２に結合された通信インターフェース３２に接続するネットワーク・リンク３４（例えば、モデムまたはネットワーク接続）経由で搬送波または他の増殖媒体に具体化されたデータ信号によって、要求コンピュータ・システム１０に送信される。通信インターフェース３２は、例えば、ローカル・エリア・ネットワーク（ＬＡＮ）、広域ネットワーク（ＷＡＮ）、あるいはここに記載されているように、直接インターネット・サービス・プロバイダー（ＩＳＰ）３７に接続されるネットワーク・リンク３４に結合している双方向のデータ通信などを提供する。具体的には、ネットワーク・リンク３４は、１つまたは複数のネットワークに対して、有線ネットワーク通信・無線ネットワーク通信の両方、あるいはそのいずれかを提供する。

【００２０】

次に、ＩＳＰ３７は、ネットワーク１０２を通じてデータ通信サービスを提供する。ネットワーク１０２は、相互通信のために送信制御プロトコル（ＴＣＰ）およびインターネット・プロトコル（ＩＰ）などの特定のプロトコルを用いるネットワークおよびゲートウェイの世界規模の集合に関する。ＩＳＰ３７とネットワーク１０２はいずれも、デジタル・データ・ストリームを搬送する電気信号、電磁信号または光信号を用いている。前記多様なネットワークを通じた信号、ならびにネットワーク・リンク３４上の通信インターフェース３２経由の信号は、コンピュータ・システム１０とやりとりするデジタル・データを搬送するが、これらは前記情報を移送する搬送波の例示的形態である。

【００２１】

コンピュータ・システム１０は、サーバ・システムとして実施される場合、一般的には、入・出力コントローラに接続された複数の周辺コンポーネント相互接続（ｐｅｒｉｐｈｅｒａｌ　ｃｏｍｐｏｎｅｎｔ　ｉｎｔｅｒｃｏｎｎｅｃｔ（ＰＣＩ））バス・ブリッジを介してアクセスできる複数の通信インターフェースを含む。このようにして、コンピュータ・システム１０により、複数のネットワーク・コンピュータへの接続が可能になる。

【００２２】

さらに、複数の周辺コンポーネントを、前記複数レベルのバス２２の１つに結合された複数のコントローラ、アダプタおよび拡張スロットに接続されたコンピュータ・システム１０に追加してもよい。例えば、音声入・出力２８はバス２２上で、結合してイネーブルされると、マイクロホンまたは他の音声あるいは口唇動作収集装置を通じて音声入力を制御するとともに、スピーカまたは他の音声予測装置を通じて音声出力を制御する。ディス

プレイ２４もまた、バス２２上で結合してイネーブルされると、視覚、触覚または他の画像表現形式を提供する。キーボード２６と、マウス、トラック・ボールまたはカーソル方向キーなどのカーソル制御デバイス３０とが、コンピュータ・システム１０へのユーザ入力のためのインターフェースとして、バス２２上で結合してイネーブルされる。本発明の別の実施形態においては、さらに入・出力周辺コンポーネントを追加してもよい。

【００２３】

当業者であれば、図１に表記された前記ハードウェアは、その実施状態に応じて相異することを理解するであろう。さらに、当業者であれば、前記記述例は、本発明に関する構造上の限定を示唆するものではないことも、理解するであろう。例えば、コンピュータ・システム１０は、個人用デジタル補助装置（ＰＤＡ）、ウェブ器具、キオスク、または電話の形態をとってもよい。

【００２４】

ここで図２を参照すると、ブロック図は、本発明の方法、システムおよびプログラムによる分散型ネットワーク・システムを表している。分散型データ処理システム１００は、本発明を実施できるコンピュータのネットワークである。分散型データ処理システム１００はネットワーク１０２を含むが、このネットワークは分散型データ処理システム１００内で接続された多様なデバイスとコンピュータとの間に通信リンクを提供するために用いられた媒体である。ネットワーク１０２は、ワイヤまたは光ファイバー・ケーブルなどの永久接続と電話接続を通じてなされる一時接続と無線送信接続とを含む。

【００２５】

前記表記例において、サーバ１０４と１０５は、ネットワーク１０２に接続される。さらに、クライアント１０８と１１０とは、ネットワーク１０２に接続され、入・出力（Ｉ／Ｏ）デバイス１０９と１１１とを通じてユーザ・インターフェースを提供する。クライアント１０８と１１０とは、例えば、パーソナル・コンピュータやネットワーク・コンピュータであってもよい。このアプリケーションの目的上、ネットワーク・コンピュータは、ネットワークに結合された任意のコンピュータであって、前記ネットワークに結合された別のコンピュータから、プログラムまたは他のアプリケーションを受信するコンピュータである。

【００２６】

分散型データ処理システム１００のクライアント／サーバ環境は、多くのネットワーク・アーキテクチャ内で実施される。例えば、ワールド・ワイド・ウェブ（Web）のアーキテクチャは、従来のクライアント／サーバ・モデル環境に追随している。「クライアント」および「サーバ」という用語は、データの要求者（前記クライアント）またはデータの提供者（前記サーバ）としてのコンピュータの一般的役割を示すために用いられている。前記ウェブ環境において、ネットスケープ・ナビゲーター™などのウェブ・ブラウザは概して、クライアント・システム１０８および１１０上にあって、サーバ１０４および１０５などのウェブ・サーバにウェブ文書（頁）を提供させる。さらに、クライアント・システム１０８と１１０ならびにサーバ１０４と１０５は各々、「クライアント」および「サーバ」として機能し、図１のコンピュータ・システム１０などのコンピュータ・システムを用いて実施することができる。また、本発明は、ダウンロードまたは通信をイネーブルするサーバ１０４および１０５に重点を置いて記述しているが、本発明は、ピア・ツー・ピア・ネットワーク通信とネットワーク１０２経由のダウンロードとを行うクライアント・システム１０８および１１０でも、実施することができる。

【００２７】

前記ウェブは、世界中のサーバ上にある全ての連結されたハイパーテキスト文書の組み合わせに関する。インターネットなどのネットワーク１０２は、クライアント・システム１０８および１１０と、サーバ１０４および１０５との間で、これらのハイパーテキスト文書を送信するためのインフラを提供している。前記ウェブ上の文書（頁）は、ハイパーテキスト・マークアップ言語（ＨＴＭＬ）または拡張マークアップ言語（ＸＭＬ）などの複数の言語で書き込みでき、サーバ１０４などのサーバの中から、特定のウェブ頁サーバ

を特定するＵｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒｓ（ＵＲＬ）および、ファイルにアクセスできるパス名によって識別でき、その結果、ハイパーテキスト転送プロトコル（ＨＴＴＰ）またはファイル転送プロトコル（ＦＴＰ）などのプロトコルを用いて前記特定のウェブ頁サーバからエンド・ユーザに送信できる。ウェブ頁はさらに、テキスト、グラフィック画像、映画ファイル、音声、ならびに前記ユーザがリンクをクリックすることによって前記ページを起動する時に実行する、Ｊａｖａアプレットおよび他の小型組み込み型ソフトウェア・プログラムを含むこともある。具体的には、複数のウェブ頁は、ともにリンクされて、ウェブ・サイトを形成してもよい。前記ウェブ・サイトは一般的には、前記ウェブ・サイトに接続されたウェブ頁の残りを検索するためのディレクトリを提供している構成上最前部のウェブ頁を経て、アクセスされる。ネットワーク１０２はインターネットに準拠して記述されているが、ネットワーク１０２は、イントラネットまたは他の利用できるネットワークの中でも動作することができる。

【００２８】

さらに、サーバ１０４および１０５は、クライアント１０８と１１０との間で通信を転送する通信ホストとして機能することもできる。例えば、サーバ１０４と１０５は、クライアント１０８と１１０との間のＥメール通信の通信ホストとして、機能することができる。例えば、クライアント１０８は、クライアント１１０を用いる受信者を対象としてメッセージを送信することができる。サーバ１０４は、クライアント１１０のためのＥメール・サーバとして機能し、クライアント１１０がクライアント１０８から発信されたＥメールを要求するまで、前記Ｅメールを保存する。説明のために、以下の例はＥメール通信を用いて実施するが、他の種類の通信を用いて、インスタント・メッセージ、テキスト・メッセージ、チャット、テレビ会議、およびネットワーク１０２を介せば利用可能になる他の形式の通信などを含む（ただし、これらに限定されない）本発明を実施することもできる。

【００２９】

ここで図３を参照すると、本発明の方法、システムおよびプログラムによるＥメール・クライアントのブロック図が表記されている。図示のように、Ｅメール・クライアント３００は、Ｅメール・リーダー３０４およびメール・デーモン３０６を含む。

【００３０】

Ｅメール・リーダー３０４はまた、ユーザに、Ｅメールを作らせ、ファイルさせ、検索させ、読み出しを行わせる。メール・デーモン３０６は、Ｅメール・クライアント３００のユーザを対象とするＥメールを受信し、前記Ｅメールをメッセージ・フォルダ３１０に保存する。メッセージ・フォルダ３１０に保存された受信Ｅメールに付着したウイルスは、前記ユーザの振りをしながら、Ｅメール・リーダー３０４を通じてＥメールを作成しようとする。前記ウイルスは、アドレス帳３１２から、前記ウイルスの作成したＥメールの受信対象者のアドレスを選択する。アドレス帳３１２は一般的には、Ｅメール・アドレスおよび連絡先情報を保存するためのデータ・ベースである。

【００３１】

Ｅメール・リーダー３０４は、メール・デーモン３０６に、特定された受信対象者に送信するメッセージを与える。メール・デーモン３０６は、前記ネットワークを介してＴＣＰ上で作動するシンプル・メール・トランスファー・プロトコル（ＳＭＴＰ）を用いて、前記メッセージを、別のマシン、一般的には前記メール・サーバ、で作動するメール・デーモンに送信するが、前記マシンは前記メッセージを、前記受信対象者によって検索が可能なメール・ボックスに入れる。

【００３２】

Ｅメールがメール・デーモン３０６によって送信される前に、前記Ｅメールをスキャンして、ウイルスを含むＥメールの送信を停止することができれば好都合である。ウイルスの送信を削減するために、複数のセキュリティ層を用いると好都合である。これらのセキュリティ層の１つは、Ｅメール・クライアント３００の中に含まれるウイルス軽減コントローラ３０２を通じて、実施される。

【００３３】
ウイルス軽減コントローラ３０２は、送信すべき各Ｅメールを、前記Ｅメールがメール・デーモン３０６に送信される前に、スキャンする。ウイルス軽減コントローラ３０２は先ず、前記Ｅメール内の受信対象者アドレス数および前記受信対象者の他の特性値を確定する。
次に、ウイルス軽減コントローラ３０２は、前記Ｅメールに添付ファイルまたは組み込みファイルがあるか否かを確定する。その後、ウイルス軽減コントローラ３０２は、受信対象者アドレスの数および他の特性値を、軽減設定ファイル３０８としてメモリに保存された複数の軽減設定と比較する。例えば、前記Ｅメール内の前記受信対象者アドレスの数が、Ｅメール毎の前記軽減設定を超える場合、前記Ｅメールは、前記ユーザが送信される前記Ｅメールを認証しない限り、メール・デーモン３０６に送信されない。阻止されたＥメールは、メッセージ・フォルダ３１０に保存され、ウイルス軽減コントローラ３０２は、ネットワーク管理者または潜在的ウイルスを監視する他のサービス機関に、通報を開始する。
【００３４】
本発明の一実施形態において、Ｅメール・クライアント３００に記載されている前記コンポーネントは、単一のコンピュータ・システム内においてアクセス可能である。しかし、本発明の別の実施形態において、Ｅメール・クライアント３００に記載されている前記コンポーネントは、分散型ネットワーク・システムの全域で、複数のコンピュータ・システムを介してアクセスすることが可能である。
【００３５】
ここで図４を参照すると、本発明の方法、システムおよびプログラムによるアドレス帳の構成要素のブロック図が図示されている。表記のように、図３のＥメール・クライアント３００のアドレス帳３１２は、保存されたＥメール・アドレスのデータ・ベースおよび他のアドレス指定情報を提供する。説明のために、アドレス帳３１２は、Ｅメール・アドレスを、ビジネス用アドレス４０２と友人アドレス４０４と家族アドレス４０６の３つのグループに分類する。アドレス帳３１２はどの種類のデータ・ベース構造を用いても、Ｅメール・アドレスを分類し保存できることが理解される。例示用として、ビジネス用アドレス４０２に保存された前記Ｅメール・アドレスの選択アドレスを参照符号４０８に表記する。
【００３６】
ここで図５を参照すると、本発明の方法、システムおよびプログラムによる前記軽減設定ファイルのブロック図が表記されている。図示のように、図３のＥメール・クライアント３００の軽減設定ファイル３０８は、保存された軽減設定のデータ・ベースを提供する。一実施形態において、軽減設定ファイル３０８は、二種類の設定即ち、ファイル毎の受信者設定５０４とメッセージ毎の受信者設定とを含む。別の実施形態においては、他の種類の設定を実施してもよい。さらに、ユーザが特定した設定に加えて、デフォルト設定を軽減設定ファイル３０８の中に設けてもよい。
【００３７】
例示用として、ファイル毎の受信者設定５０４として保存されたユーザ特定設定の選択を参照符号５０８に表記する。ファイル毎の受信者設定５０４は、ファイルが添付されているか、または中にファイルが組み込まれているＥメールと関連した設定を含む。参照符号５０８で表示された前記選択において、３つの設定例が例示されている。最初の２つの例は、百分率に基づく最大許容値設定である。最初に、前記アドレス帳で最大４０％の前記アドレスを設定する。次いで、前記アドレス帳で最大３３％の前記ビジネス用アドレスを設定する。さらに、ファイルの種類ごとに上限を設定する。例えば、　．ｄｏｃファイルについては、最大４つのアドレスを設定する。本発明の別の実施形態においては、ファイルを含む全てのＥメールについて、他の値を最大許容値に設定してもよい。
【００３８】
さらに、例示用として、メッセージ毎の受信者設定として保存されているユーザ指定設

定の選択を、参照符号５１０に表示する。メッセージ毎の受信者設定５０６は、全てのＥメールと関連した設定を含む。参照符号５１０に表示された前記選択において、３つの設定例が例示される。１番目に、前記アドレス帳の前記アドレスの百分率に基づいて、最大許容値が設定される。２番目に、複写（ｃｃ）の受信者である受信者の最大数が設定される。第３に、受信者総数の最大数が設定される。本発明の別の実施形態においては、他の値を全てのＥメールについて最大許容値に設定してもよい。

【００３９】

軽減設定ファイル３０８内に設定された値は、前記ユーザによって設定されてもよいし、ネットワーク管理者またはウイルス検出サービス機関によって離れて設定されてもよい。さらに、ウイルス軽減コントローラ３０２は、特定のユーザの一般的な使用を監視し、その使用に応じて、軽減設定ファイル３０８を設定してもよい。

【００４０】

ここで図６を参照すると、本発明が適用される添付ファイル付きＥメールの説明図が表記されている。前記例に図示されているように、添付ファイル６００付きのＥメールは、参照符号６０２で表記された前記Ｅメール・アドレスに送信されるＴｏｍ　Ｊｏｎｅｓによって構成されている。前記例において、参照符号６０２で表示された前記Ｅメール・アドレスを、図４の参照符号４０８で表示された前記ビジネス用Ｅメール・アドレスと比較すると、他のＥメール・アドレスは全て、添付ファイル６００付きＥメールの対象とするアドレスとして含まれていることが明らかである。添付ファイル６００付きＥメールは、ウイルスがアドレス帳のアドレスの全てではないが、その内のあるものを選択して示す行為の一例を表わす。さらに、添付ファイル６００付きＥメールは、ウイルスが、参照符号６０４で表記されるようなファイルを添付することによって示す行為の一例を表わす。表記されていないが、ウイルスは前記ファイルを添付する代わりに、添付ファイル６００付きＥメール内に前記ファイルを組み込むこともできる。

【００４１】

ユーザの添付ファイル６００付きＥメール送信の要求に応答して、前記ウイルス軽減コントローラは望ましくは、添付ファイル６００付きＥメールをスキャンして、前記最大アドレス指定制限のいずれかを超えているか確定する。最初に、前記ウイルス軽減コントローラは、前記作成された添付ファイル６００付きＥメールの、対象とするＥメール・アドレスの数および他の特性値を計算する。さらに、前記ウイルス軽減コントローラは、前記対象とするＥメール・アドレスを、前記アドレス帳の前記ビジネス用アドレスと比較して、Ｅメール６００に含まれるビジネス用アドレスの数を確定する。次に、前記ウイルス軽減コントローラは、対象とするＥメール・アドレスの数および前記対象とするEメール・アドレスの他の特性値を、前記最大アドレス指定の設定と比較する。図５の参照符号５０８で表記されているような前記設定制限によれば、対象とするＥメール・アドレスの数は、参照符号６０４で表記されているように、添付された．ｄｏｃファイルの前記最大数のアドレス（２）を超える。さらに、図５の参照符号５０８で表記されているように、設定された前記制限によれば、対象とするＥメール・アドレスの数は、前記ビジネス用アドレスの前記最大百分率（３３％）を超える。上記例においては、添付ファイル６００付きＥメールの対象とするアドレスの数は、図５の参照符号５１０で示されているようにメッセージ毎に設定された前記制限を越えないが、別の実施形態においては、添付ファイル付きのＥメール・メッセージは、ファイル基準の制限とメッセージ別基準の制限とを超える場合もある。

【００４２】

ここで図７を参照すると、本発明が適用されるＥメールの説明図が表記されている。前記例に表記するように、Ｅメール７００は、参照符号７０２および７０４で表記された前記Ｅメール・アドレスに送信されるＴｏｍ　Ｊｏｎｅｓによって構成されている。前記例において、参照符号７０２および７０４で表記された前記Ｅメール・アドレスを、図４の参照符号４０８で表記された前記ビジネス用Ｅメール・アドレスと比較すると、前記ビジネス用Ｅメール・アドレスは全て、Ｅメール７００の対象アドレスとして含まれているこ

とが明らかである。Ｅメール７００は、ウイルスが前記Ｅメールを先ず前記送信者に送信した後、前記アドレス帳の前記アドレスの残りを複写することによって示す行為の一例を表す。ここで、Ｅメール７００は、参照符号７０２で表記されているように、前記送信者、Ｔｏｍ　Ｊｏｎｅｓに先ず送信され、前記全てのビジネス用Ｅメール・アドレスに複写される。

【００４３】

ユーザのＥメール７００送信の要求に応答して、前記ウイルス軽減コントローラは望ましくは、Ｅメール７００をスキャンして、前記最大アドレスの指定制限のうち、いずれかの制限を超えているか否か確定する。最初に、前記ウイルス軽減コントローラは、前記作成されたＥメール７００の対象Ｅメール・アドレスの数を計算する。前記例において、前記対象とするＥメール・アドレスの前記特性値は、前記対象とするＥメール・アドレスの各アドレスの総数および前記複写されたＥメール・アドレスの総数を含む。次に、前記ウイルス軽減コントローラは、前記対象とするＥメール・アドレスの数を、前記最大アドレス設定と比較する。図５の参照符号５１０で表記されているように、設定された前記制限によれば、対象とするＥメール・アドレスの前記ｃｃ受信者の数は、参照符号６０４で表記されるｃｃ受信者（５）の前記最大数を超える。

【００４４】

ここで図８を参照すると、本発明の方法、システムおよびプログラムによる認証ウインドウの説明図が表記されている。Ｅメールが送信される前に、前記ウイルス軽減コントローラが、前記Ｅメールの前記最大アドレス指定の制限を超えていると確定した場合、送信者認証要求ウインドウ８００または他の形態の送信者認証要求が開始される。例えば、図６および図７に示された前記Ｅメールの送信要求に応答して、認証要求が開始される。

【００４５】

前記Ｅメールを送信する前に、さらなる手入力または口頭入力による認証を提供するよう送信者に要求する追加ステップは、Ｅメール・ウイルスの前記増殖の軽減に役立つであろう。このような要求の例として、送信者は、参照符号８０２に表記されているように、前記最大許容値を超えていることを示すメッセージで促される。その後、送信者は、前記Ｅメールを認証するために、入力ブロック８０４においてパスワードを入力するように促される。別の実施形態において、前記送信者は、ボタンを選択するか、他の入力を提供するかのみ要求される場合もある。さらに、別の実施形態において、前記送信者に出力された前記メッセージは、前記特定の最大許容値を超えていることを示すことができる。さらに、別の実施形態において、各制限を超える毎に、別個の要求をすることもできる。

【００４６】

ここで図９を参照すると、本発明の方法、システムおよびプログラムにより、Ｅメール・ウイルスの送信を軽減するプロセスおよびプログラムの高レベルの論理フローチャートが表示されている。表記のように、前記プロセスは、ブロック９００でスタートし、その後、ブロック９０２に続く。ブロック９０２は、Ｅメールの送信要求が受信されたか否かについて確定することを表わす。前記プロセスは、Ｅメールの送信要求が受信されるまで、ブロック９０２において反復し、その後、前記プロセスはブロック９０４へ続く。ブロック９０４は、前記受信対象者の数を計算することを表している。具体的には、前記受信対象者の複数の特性値が計算されるが、前記特性値には、全ての受信対象者、全ての主要な受信対象者、全ての複写送付先の受信対象者、特定のメール・プロバイダへの全ての受信者アドレス、最大許容値を超えるか否かを計算するために必要な他のカテゴリ等が含まれるが、これらに限定されない。加えて、最大許容値が、そのアドレスが前記アドレス帳にも記載されている前記受信対象者の数に基づいている場合、前記受信対象者とアドレス帳との比較は、前記受信対象者の前記特性値を確定するのにも必要となる。

【００４７】

次に、ブロック９０６は、ファイルが前記Ｅメールに添付されているか、組み込まれているかについて確定することを表す。ファイルが前記Ｅメールに添付されているか、組み込まれている場合、前記プロセスはブロック９０７へ続く。具体的には、Ｅメールにファ

イルが組み込まれているか、またはＥメールにコピーされている場合、フラグが好適に設定されるが、前記フラグは、ブロック９０６によって表記される前記プロセスのステップにおいて、その後検出される。ブロック９０７は、前記受信対象者の数と、前記ファイルの前記最大許容値とを比較することを表し、前記プロセスは、ブロック９０８へ続く。

【００４８】

ブロック９０６に戻って、ファイルが前記Ｅメールに添付されていないか、組み込まれていない場合、前記プロセスは、ブロック９０８へ続く。ブロック９０８は、前記受信対象者の数と、単一のＥメールの前記最大許容値とを比較することを表す。その後、ブロック９１０は、前記受信対象者の数が前記最大許容値を超えているか否か確定することを示す。前記受信対象者の数が前記最大許容値を超えない場合、ブロック９１２に示されるように、前記Ｅメールは、前記メール・デーモンに転送され、前記プロセスが終了する。しかし、前記受信対象者の数が前記最大パラメータを超えている場合、前記プロセスはブロック９１４に続く。

【００４９】

ブロック９１４は、前記Ｅメールの送信のために送信者認証を要求することを表している。この認証は、前記送信者に、マウス・クリックまたはキーストロークなどの手入力によってパスワードの入力または前記送信認証の入力のみを行うことを要求するものである。望むらくは、ウイルスに容易に改ざんされないような入力が必要である。次に、ブロック９１６は、前記送信者が前記Ｅメールの送信を認証したか否かについて確定することを表している。前記送信者が前記Ｅメールの送信を認証した場合、前記プロセスはブロック９１２へ続く。前記送信者が前記Ｅメールの送信を認証しない場合、前記プロセスはブロック９１８へ続く。ブロック９１８は、前記Ｅメールを保存することを表している。その後、ブロック９２０は、Ｅメールが阻止されている旨を前記ネットワーク管理者に通報することを示し、前記プロセスは終了する。

【００５０】

本発明については、完全に機能するデータ処理システムの文脈において記述してきたが、当業者であれば、本発明の前記プロセスは、コンピュータ読み出し可能な媒体形式の指令および多様な形式の指令で配信することが可能であり、且つ、本発明は、前記配信を実施するために実際に用いられる前記特定の種類の信号搬送媒体に関わりなく、平等に適用されると理解することに留意することが重要である。コンピュータ読み出し可能な媒体の例を挙げると、フロッピー・ディスク、ハード・ディスク・ドライブ、ＲＡＭ、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭなどの記録可能型媒体や、デジタル通信リンクおよびアナログ通信リンクなどの送信用媒体、例えば高周波送信および光波送信などの送信形式を用いた有線通信リンクや無線通信リンクがある。コンピュータで読み出し可能な媒体は、特定のデータ処理システムにおいて実際に使用するために復号化された、コード化形式の形態をとることができる。

【００５１】

前記発明について、具体的に図示および好適な実施形態を参照して記述してきたが、当業者であれば、形態および細部についての種々の変更が、前記発明の範囲から逸脱することなくなし得ることを理解するであろう。

【図面の簡単な説明】

【００５２】

【図１】図１は、本発明の方法、システムおよびプログラムが実施されるコンピュータ・システムを表すブロック図である。

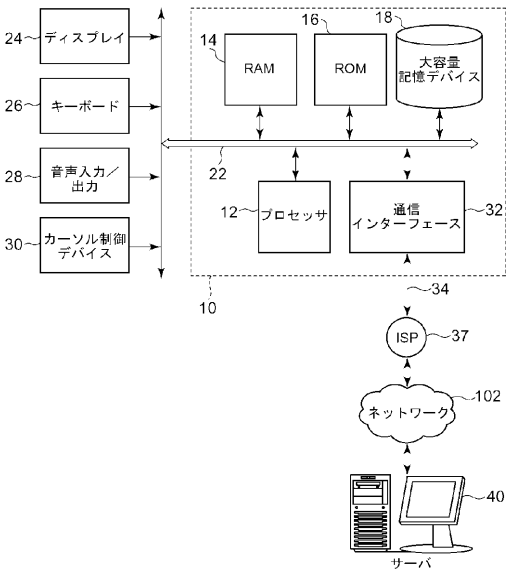
【図２】図２は、本発明の方法、システムおよびプログラムによる分散型ネットワーク・システムを表すブロック図である。

【図３】図３は、本発明の方法、システムおよびプログラムによるＥメール・クライアントを表すブロック図である。

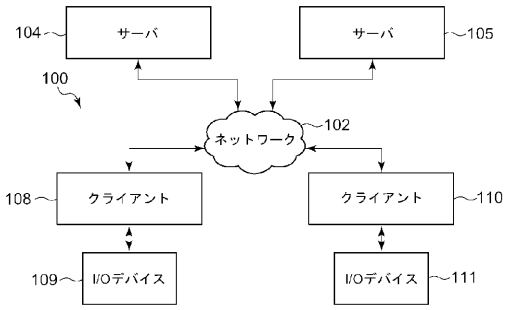
【図４】図４は、本発明の方法、システムおよびプログラムによるアドレス帳を表すブロック図である。

【図５】図５は、本発明の方法、システムおよびプログラムによる軽減設定を表すブロック図である。
【図６】図６は、本発明が適用できる添付ファイル付きＥメールの説明図である。
【図７】図７は、本発明が適用できるＥメールの説明図である。
【図８】図８は、本発明の方法、システムおよびプログラムによる認証ウインドウの説明図である。
【図９】図９は、本発明の方法、システムおよびプログラムによるＥメール・ウイルス送信を軽減するプロセスおよびプログラムの、高レベルの論理フロー・チャートである。

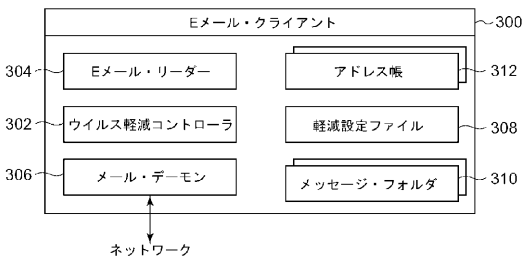
【図１】



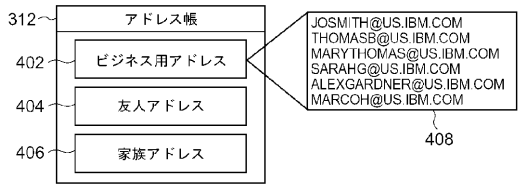
【図２】



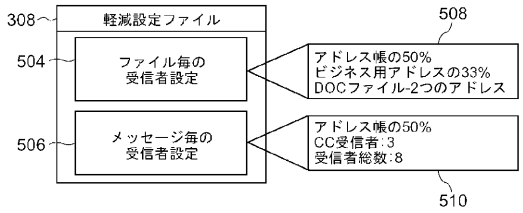
【図３】



【図４】

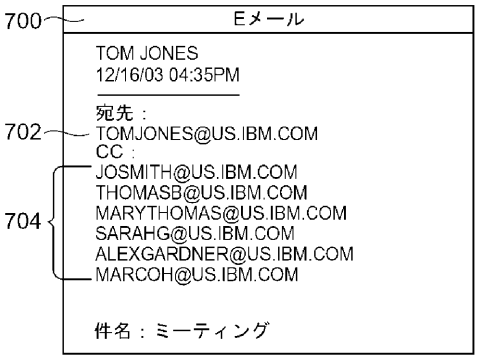


【図５】

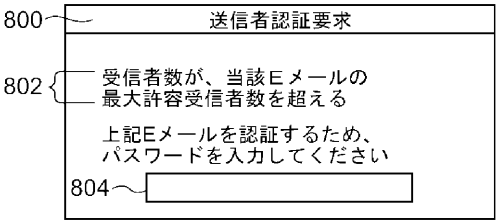


【図６】

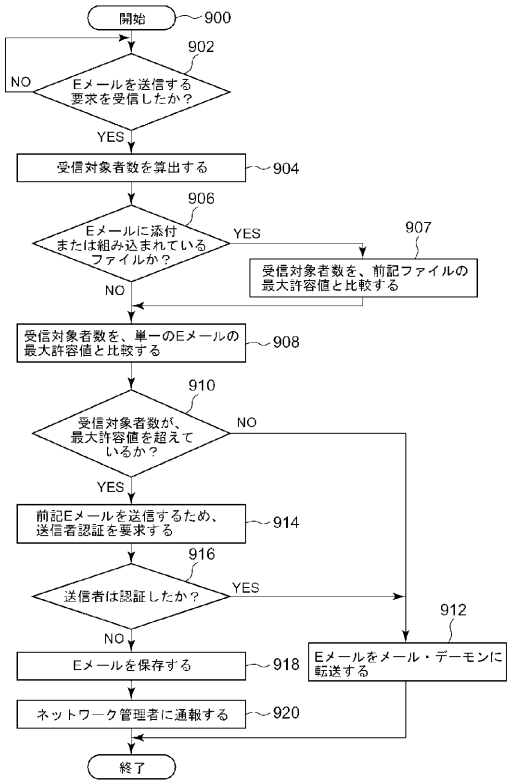
【図７】



【図８】



【図９】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2004/052153

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/22 H04L12/58 G06F1/00

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)
IPC 7 H04L G06F

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, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 1 280 039 A (NETWORKS ASSOC TECH INC) 29 January 2003 (2003-01-29) paragraphs [0005] - [0007], [0013], [0017], [0019], [0021], [0026] figure 3	1-24
P,X	US 2004/103159 A1 (WILLIAMSON MATTHEW MURRAY ET AL) 27 May 2004 (2004-05-27) paragraphs [0009], [0010], [0017], [0080] - [0085], [0087]	1-24
P,X	EP 1 369 766 A (HEWLETT PACKARD DEVELOPMENT CO) 10 December 2003 (2003-12-10) claims 1,32	1,2,9, 10,18-20

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in 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
27 January 2005	20/01/2005

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	Lázaro, M.L.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2004/052153

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1280039 A	29-01-2003	US 2003023875 A1	30-01-2003
		EP 1280039 A2	29-01-2003
US 2004103159 A1	27-05-2004	GB 2391419 A	04-02-2004
		EP 1369766 A2	10-12-2003
EP 1369766 A	10-12-2003	GB 2391419 A	04-02-2004
		GB 2394382 A	21-04-2004
		GB 2401280 A	03-11-2004
		EP 1369766 A2	10-12-2003
		US 2004103159 A1	27-05-2004
		EP 1411703 A2	21-04-2004
		US 2004083372 A1	29-04-2004
		US 2004218327 A1	04-11-2004

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,IT,LU,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,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,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．フロッピー
２．ＪＡＶＡ

(74)代理人 100112690
弁理士 太佐 種一
(72)発明者 ジルアード、ジャニス、マリー
アメリカ合衆国７８７５０ テキサス州オースティン ペイントブラッシュ・ホロー６８０８
(72)発明者 ラトリフ、エミリー、ジェーン
アメリカ合衆国７８７５８ テキサス州オースティン ウィロー・ベンド・ドライヴ１２３２１