(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3931908号
(P3931908)
(45)発行日　平成19年6月20日(2007.6.20)　(24)登録日　平成19年3月23日(2007.3.23)

(51)Int.Cl.		F I		
H04L 12/58	(2006.01)	H04L	12/58	100F
G06F 13/00	(2006.01)	G06F	13/00	610S

請求項の数 7　(全 18 頁)

(21)出願番号	特願2005-78368(P2005-78368)
(22)出願日	平成17年3月18日(2005.3.18)
(62)分割の表示	特願2001-334874(P2001-334874)の分割
原出願日	平成13年10月31日(2001.10.31)
(65)公開番号	特開2005-237023(P2005-237023A)
(43)公開日	平成17年9月2日(2005.9.2)
審査請求日	平成17年4月14日(2005.4.14)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　片岸　誠
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所　デジタルメディア開発本部内
(72)発明者　佐野　賢治
神奈川県横浜市戸塚区吉田町２９２番地
株式会社日立製作所　デジタルメディア開発本部内

最終頁に続く

(54)【発明の名称】電子メールシステム、メールサーバ及びメール端末

(57)【特許請求の範囲】

【請求項１】

メールサーバを介して電子メールを受信する受信手段と、

前記受信手段により受信した電子メールを保存する記憶手段と、

前記受信手段により受信した電子メールがウイルスに感染しているとき、前記ウイルスの種類に応じて前記電子メールを前記記憶手段に保存するか否かを制御する制御手段と、

を備えていることを特徴とするメール端末。

【請求項２】

前記制御手段は、前記ウイルスの種類が古いとき、前記電子メールを前記記憶手段に保存するように制御することを特徴とする請求項１に記載のメール端末。

【請求項３】

前記制御手段は、前記ウイルスが発動による悪影響を発生しない種類のものであるとき、前記電子メールを前記記憶手段に保存するように制御することを特徴とする請求項１に記載のメール端末。

【請求項４】

請求項１ないし３のいずれかに記載の前記メール端末は、前記記憶手段に保存された電子メールの転送指示をユーザが入力する操作手段を備え、

前記制御手段は、前記操作手段により転送を指示された電子メールがウイルスに感染しているとき、前記ユーザにより指定された転送先に応じて転送あるいは転送を禁止するように制御することを特徴とするメール端末。

【請求項５】
請求項４に記載の制御手段は、前記ユーザにより指定された転送先がウイルス検査可能な装置であるとき、前記電子メールを転送することを特徴とするメール端末。
【請求項６】
請求項４または５に記載の制御手段は、前記ユーザにより指定された転送先が他のメール端末であるとき、前記電子メールの転送を禁止することを特徴とするメール端末。
【請求項７】
請求項１ないし６のいずれかに記載のメール端末とメールサーバとを備えてなる電子メールシステムであって、
前記メールサーバは、電子メールの管理を行うメール処理手段と、前記メール処理手段を介して受信された電子メールを記憶するメール記憶手段と、前記受信された電子メールがコンピュータウイルスに感染しているか否かを判定するウイルス判定手段と、前記ウイルス判定手段によるウイルス感染の判定結果を前記電子メールに付加する情報付加手段と、前記ウイルス判定手段により前記電子メールがウイルスに感染していると判定された場合には、前記電子メールの受信者への課金処理を中止する課金管理手段と、を備えていることを特徴とする電子メールシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子メールシステム、メールサーバ及びメール端末に関する。
【背景技術】
【０００２】
電子メールシステムは、大略すると、メールサーバとメールクライアント（電子メールソフトウエア）とから構成される。メールサーバは、通常各ドメイン毎に設置されるもので、例えば、インターネットサービスプロバイダーや携帯電話事業者等がネットワーク上に設置する。ユーザは、例えば、パーソナルコンピュータや携帯電話あるいは携帯情報端末（ＰＤＡ）等のような、メールクライアントが稼働するメール端末を使用して、メールサーバとの間で電子メールの送受信を行う。
【０００３】
あるユーザ（発信者）が他のユーザ（受信者）に電子メールを送信する場合、発信者が発信した電子メールは、例えば、SMTP（Simple Mail Transfer Protocol）のようなメール転送プロトコルを用いて、宛先ドメインのメールサーバに送られる。メールサーバには各ユーザ毎に専用のディレクトリ（メールボックス）が予めそれぞれ用意されており、メールサーバに到着した電子メールは、各宛先のメールボックスに仕分けされて保存される。電子メールを受信する場合、メールクライアントは、例えば、POP3（Post Office Protocol Version 3）のようなメール受信プロトコルを用いて、メールボックスから電子メールを取り出し、メール端末内に取り込む。電子メールのフォーマットは、例えば、MIME（Multipurpose Internet Mail Extensions）により拡張されており、これにより、画像ファイルや音楽ファイルあるいはプログラムファイル等のバイナリファイルをテキストに添付することができるようになっている。
【０００４】
ところで、電子メールシステムの普及に伴って、電子メールを介したコンピュータウイルス（以下、「ウイルス」と略記）の被害も増加する傾向にある。例えば、電子メールに添付されたバイナリファイル中にウイルスが含まれている場合、ユーザがメール閲覧時に添付ファイルを実行すると、ウイルスが端末のシステム内に侵入等して、データ破損等の種々の不具合を発生させる。
【０００５】
このため、例えば、特開２００１－１３４４３３号公報等に記載されているように、ウイルスを発見して駆除するという、いわゆるワクチンソフトウエアをメール端末に搭載し、このワクチンソフトウエアによって、受信した電子メールがウイルスに感染しているか

否かを検査する技術が既に知られている。ワクチンソフトウエアでは、例えば、添付ファイルの情報パターンを既知のウイルスパターンと比較照合することによってウイルスを発見し、ユーザに警告等するようになっている。

【０００６】

【特許文献１】特開２００１－１３４４３３号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

前記公報に示されているように、メール端末内でウイルス感染の有無を検査する従来技術には、以下に述べるような問題点がある。まず、ユーザは、常に最新のウイルスパターンを入手する必要があり、手間がかかる。コンピュータウイルスは日々変化しており、世情を騒がせたウイルスの亜種が幾つも発生することがある。従って、メール端末内のウイルスパターンを常に最新のものに更新していなければ、これら未知の新しいウイルスに対抗することができず、ウイルスパターンの更新に手間がかかる。

【０００８】

次に、メール端末内でウイルス感染を検査する場合、ワクチンソフトウエアのコードサイズ及びアルゴリズムやウイルスパターンデータのデータサイズ等によって相違するが、メール端末のコンピュータ資源（ＣＰＵ実行時間やメモリ）を消費する。従って、搭載されたＣＰＵの処理能力が低く、利用可能なメモリ量も少ないメール端末の場合は、ウイルス検査を自機内で行うことの負担が大きい。

【０００９】

特に、近年では、携帯電話や携帯情報端末のような比較的小型で持ち運び容易なメール端末が広く普及しているが、これら小型のメール端末は、卓上型のパーソナルコンピュータ等に比較して、その物理的サイズや消費電力等の観点からＣＰＵ処理能力やメモリ量に大きな制限を受けている。従って、コンピュータ処理能力が乏しい小型のメール端末内でウイルス検査を実行すると、ウイルス検査に長時間を要する上に消費電力も増大し、現実的ではない。

【００１０】

また、ウイルスパターンを更新するために、小型のメール端末を外部サーバに接続させると、ユーザに課金が発生し、ユーザの不満が増大する。

【００１１】

本発明は、上述した種々の問題に鑑みてなされたもので、その目的は、メール端末の外部で事前にウイルス感染の判定を行い、メール端末側での負担を少なくし、使い勝手を向上できるようにした電子メールシステム、メールサーバ及びメール端末を提供することにある。本発明の他の目的は、コンピュータ処理能力等に制限を受ける小型のメール端末に適したウイルス検査を行うことができる電子メールシステム、メールサーバ及びメール端末を提供することにある。本発明の更なる目的は、後述する実施の形態の記載から明らかになるであろう。

【課題を解決するための手段】

【００１２】

本発明に係るメール端末は、メールサーバを介して電子メールを受信する受信手段と、前記受信手段により受信した電子メールを保存する記憶手段と、前記受信手段により受信した電子メールがウイルスに感染しているとき、前記ウイルスの種類に応じて前記電子メールを前記記憶手段に保存するか否かを制御する制御手段とを備える。また、メールサーバは、電子メールの管理を行うメール処理手段と、前記メール処理手段を介して受信された電子メールを記憶するメール記憶手段と、前記受信された電子メールがコンピュータウイルスに感染しているか否かを判定するウイルス判定手段と、前記ウイルス判定手段によるウイルス感染の判定結果を前記電子メールに付加する情報付加手段と、前記ウイルス判定手段により前記電子メールがウイルスに感染していると判定された場合には、前記電子メールの受信者への課金処理を中止する課金管理手段を備える。

【発明の効果】
【００３４】
本発明によれば、ユーザの使い勝手を向上しつつ、メール端末の安全性を向上させることができる。
【発明を実施するための最良の形態】
【００３５】
本実施形態に係る電子メールシステムは、下の特徴を有するメールサーバとメール端末とを含んで構成される。
メールサーバは、到着した電子メールがコンピュータウイルスに感染しているか否かを判定するウイルス判定手段と、ウイルス判定手段によるウイルス感染の判定結果を電子メールに付加する情報付加手段と、を含んで構成されている。一方、メール端末は、メールサーバから受信された電子メールに付加された判定結果に基づいて、ウイルス感染に関する情報をユーザに提供する情報提供手段を含んでいる。例えば、各ドメイン毎に設置されるメールサーバは、複数のメール端末との間で電子メールの送受信を行うことができるようになっている。メールサーバに到着した電子メールは、ウイルス判定手段によっていわゆるコンピュータウイルスに感染しているか否かが判定（検査）される。ここで、コンピュータウイルスとは、例えば、端末に記憶されている記憶内容を消去したり、書き換えたり、外部へ転送したり等のような、他人のコンピュータプログラムやデータに悪影響を及ぼす可能性のあるプログラムを言う。
ウイルスに感染しているか否かの判定結果は、情報付加手段によって電子メールに付加される。好ましくは、電子メールのヘッダ部に判定結果が追記される。ヘッダ部には、メールの送信者、受信者、経路、日付等の電子メールの各種属性が記載されているので、この中に判定結果を含めることにより、ヘッダを読み込むだけで電子メールが感染しているか否か、誰から送られたメールか等を容易に知ることができる。なお、好適な実施形態に示すように、ウイルス感染の有無に限らず、例えば、感染したウイルスの名称、種類、特徴、対処法等の他の情報を判定結果と共に検査情報として電子メールに付加してもよい。判定結果の付加された電子メールは、各メールアドレス毎に用意されたメールボックスに格納され、メールボックスを介してメール端末に送られる。
メール端末がメールサーバから電子メールを受信すると、情報提供手段は、電子メール中に付加された判定結果を検査し、ウイルス感染に関する情報をユーザに提供する。ここで、ウイルス感染に関する情報としては、例えば、「ウイルスに感染していることを示す警告」を挙げることができる。これに限らず、電子メールに付加されている情報がウイルスの種別や対処法も含んでいる場合には、これらウイルス種別や対処法も併せてユーザに提供することができる。なお、ウイルスに感染している事のユーザへの警告は、警告メッセージの表示に限らない。メール端末が光や音あるいは機械的振動等を発生させる他の手段を備えている場合は、例えば、ランプを点滅させたり、ブザーを鳴動させたり、端末本体を振動させたりすることにより、ユーザに警告を発することもできる。メールサーバ側でウイルス感染の判定を行い、判定結果を電子メールに付加するため、メール端末ではウイルス感染の検査を行う必要がなく、メール端末のユーザがウイルスパターンの更新作業等を行う必要が無くなる。メール端末は、さらに、判定結果に基づいて、受信された電子メールがウイルスに感染している場合には、該電子メールへの操作を制限する操作制限手段を備えてもよい。
操作制限手段は、例えば、ウイルスに感染した電子メールの内容表示を制限することができる。ここで、電子メールの内容表示の制限とは、ウイルスによる悪影響を未然に防止するために電子メールの閲覧を制限する意味である。従って、例えば、メール本文にはウイルスが感染しておらず、添付ファイルにのみウイルスが存在するような場合は、添付ファイルの実行のみを制限し、メール本文の表示は許可してもよい。これにより、ウイルスに感染した電子メールをメール端末が受信した場合でも、ウイルスの発動を防止して被害を未然に食い止めることができる。操作制限手段は、ウイルスに感染した電子メールを他の端末に転送することを制限するものであってもよい。なお、「転送」には、いわゆる返

信も含まれる。ウイルスに感染した電子メールの転送を制限することにより、ウイルスが他のメール端末に伝染するのを防止できる。

さらに、操作制限手段は、ウイルスに感染した電子メールを、予め設定された所定の装置に対してのみ転送を許可し、他の端末への転送を制限してもよい。ここで、予め設定された所定の装置としては、例えば、ウイルスを検査するための装置（一例として、ウイルス検査プログラムを搭載したパーソナルコンピュータ）等を挙げることができる。所定の装置への転送は、ウイルス感染の有無にかかわらず行うことができ、これにより、ウイルスの調査等を行うことができる。

なお、「予め設定された所定の装置」を、「外部ネットワークを介さずにメール端末に直接的に接続された装置」として捉えることもできる。転送に用いるインターフェースの種類を検出することによって、外部ネットワーク（メールサーバ）を経由した転送は禁止し、メール端末に直接的に接続されたパーソナルコンピュータ等にのみ転送を許可するように構成することができる。

また、メールサーバは、ウイルス判定手段によって電子メールがウイルスに感染していると判定された場合には、ウイルスによって悪影響が生じないように電子メールを部分的に削除することができる。メールサーバは、ウイルスの発動による悪影響が生じないように、ウイルスの全体を削除することもできるし、ウイルスを無力化する程度に部分的にウイルスを削除することもできる。安全性確保の視点で削除範囲を決定することができる。

電子メールシステムでは、メールサーバは、さらに、ウイルス判定手段によって電子メールがウイルスに感染していると判定された場合には、該電子メールのヘッダ部だけを先に送信し、メール端末から送信要求があったときには電子メールの全体をメール端末に送信するものであり、メール端末は、メールサーバから先に送信されたヘッダ部に係る電子メールの受信をユーザが希望した場合に、電子メールの送信をメールサーバに要求するように構成することができる。

電子メールがウイルスに感染している場合、メールサーバは、まず最初に電子メールのヘッダ部だけを先にメール端末に送信する。ユーザがウイルスに感染した電子メールの受信を希望する場合は、電子メールの全体を送信する。

また、電子メールシステムでは、メールサーバに、さらに、電子メールサービスに関する課金を管理する課金管理手段を備え、課金管理手段は、ウイルス判定手段によって電子メールがウイルスに感染していると判定された場合には、該ウイルスに感染している電子メールの受信者への課金処理を中止するようにしている。なお、ウイルスに感染した電子メールの受信者に対する課金を免除するに止まらず、ウイルス感染メールを発信した送信者に対して課金するようにしてもよい。

なお、本発明は、メールサーバ、メール端末、コンピュータプログラムの観点からも把握することができる。

以下、図１～図１６に基づき、本発明の実施の形態を説明する。

【実施例１】

【００３６】

図１～図７は本発明の第１の実施の形態に係り、図１は、電子メールシステムの全体構成を概略的に示す構成説明図である。

【００３７】

例えば、携帯電話事業者が設置するメールサーバ１０は、制御部１１，メール処理部１２，メール記憶部１３，検査情報付加部１４，ウイルス判定部１５及びウイルス情報記憶部１６を備えて構成されている。

【００３８】

制御部１１はメール処理部１１等を制御するものであり、メール処理部１２はメール端末２０との間の電子メール送受信処理等を行うものである。メール記憶部１３は到着した電子メールを保存するものであり、検査情報付加部１４は、後述の検査情報を電子メールのヘッダに付加するものである。ウイルス判定部１５は、ウイルス情報記憶部１６に予め記憶されたウイルスパターンに基づいて、電子メールがコンピュータウイルスに感染して

いるか否かを判定するものである。

【００３９】

メールサーバ１０はインターネット３１に接続されており、インターネット３１を介して他の端末（図示せず）からの電子メールがメールサーバ１０に到着する。メールサーバ１０に到着した電子メールは、所定のウイルス検査を受けた後で、メール記憶部１３に記憶される。メールサーバ１０に保存された電子メールは、例えば、携帯電話の基地局３２から無線通信を介してメール端末２０に送信される。

【００４０】

メール端末２０は、例えば、携帯電話や携帯情報端末等のような小型の端末として構成されている。本実施形態では、インターネットメールの送受信機能を備えた携帯電話をメール端末２０として採用する。

【００４１】

メール端末２０は、制御部２１，メール処理部２２，メール記憶部２３，表示部２４，報知部２５，操作部２６を備えている。

【００４２】

制御部２１は、メール処理部２１等を制御するものである。メール処理部２２は、操作部２６からの入力に応じて電子メールの送受信処理等を行うものである。メール記憶部２３は、メールサーバ１０から受信した電子メールを保存するものであり、記憶装置としては、例えば、不揮発性メモリなどが用いられる。表示部２４は、例えば、液晶ディスプレイ装置やプラズマディスプレイ装置等として構成され、電子メールの内容やメール端末の状態（例えば、電波強度やバッテリー残量）等を表示するものである。

【００４３】

報知部２５は、電子メールの着信を、例えば、光、音、振動等によってユーザに報知するものである。光と音、音と振動、光と振動等のように２種類以上の刺激で、電子メールの着信を報知させることもできる。また、ウイルスに感染していない電子メールが着信した場合（正常時）と、ウイルスに感染した電子メールが着信した場合（異常時）とで、報知内容を違えることができる。例えば、正常時の電子メール着信音よりも異常時の着信音を大きくしたり、音色を変えたりすることができる。あるいは、正常時の着信振動と異常時の着信振動の周波数や強さを変えることもできる。

【００４４】

図２は、電子メールの構成及び検査情報の付加位置等を示す模式図である。電子メールは、大別すると、ヘッダＭ１と、本文Ｍ２と、添付ファイルＭ３とから構成されており、メールサーバ１０のウイルス判定部１５による判定結果を含む検査情報Ｍ１１は、ヘッダＭ１内に追加される。検査情報が付加された電子メールは、２種類の方法でメール端末２０に配送される。一つの方法は、電子メール全体をメール端末２０に送信する方法であり（図２中の「Ａ」）、他の一つの方法は、電子メールのヘッダＭ１だけを先にメール端末２０に送信し、ユーザの指示を待ってから電子メールの全体を送信する方法である（図２中の「Ｂ」）。本実施の形態では、電子メールの全体を最初から送信する場合を説明し、後の実施形態でヘッダＭ１を先に送信する場合を説明する。

【００４５】

図３は、ヘッダの構成を示す説明図である。ヘッダには、例えば、返信先アドレス（Return-Path）、発信日時（Date）、差出人メールアドレス（From）、受信者メールアドレス（To）、経路情報（Received）、メッセージ識別名（Message-ID）、メールタイトル（Subject）等の書誌的情報が記載されている。本実施の形態では、このヘッダＭ１内に、検査情報Ｍ１１を追加する。検査情報Ｍ１１には、例えば、ウイルス感染の判定結果、ウイルス情報（ウイルス名や種類等）、ウイルスへの対処法等を含めることができる。従って、メール端末２０側では、ヘッダＭ１のみを検査することにより、検査情報Ｍ１１を容易に検出することができる。

【００４６】

次に、図４～図７に基づいて、本実施の形態の作用を説明する。なお、図中では、ステ

ップを「Ｓ」と略記する。

【００４７】

図４のフローチャートは、メールサーバ１０及びメール端末２０でそれぞれ行われる処理の全体概要を示す。

【００４８】

メールサーバ１０では、インターネット３１を介して電子メールが到着すると（S101:YES）、この電子メールについてウイルス判定を行う（S102）。ウイルスに感染しているか否かの判定が終了すると、上述した内容の検査情報Ｍ１１がヘッダＭ１内に記述される（S103）。検査情報Ｍ１１が付加された電子メールは、メールの宛先に応じてメール記憶部１３に保存され（S104）、メール端末２０に配信される（S105）。なお、メール端末２０からの要求を待ってメールサーバ１０からメールを配信することもできるし、メール端末２０の要求を待たずにメールサーバ１０から配信することもできる。

【００４９】

メール端末２０では、メールサーバ１０から電子メールを受信すると（S201:YES）、受信した電子メールをメール記憶部２３に保存する（S202）。次に、メール端末２０は、ヘッダＭ１から検査情報Ｍ１１を検出し、ウイルス感染の有無等を報知部２５を介してユーザに報知すると共に、検査情報Ｍ１１の内容を表示部２４を介して表示させる（S203）。報知の方法としては、例えば、ウイルス判定結果に応じて報知音を変えたり、点滅間隔や点滅パターン、点灯色等をウイルス判定結果に応じて変えたりすることにより、行うことができる。あるいは、振動による報知の場合は、振動の間隔やパターン等をウイルス判定結果に応じて変えても良い。

【００５０】

受信した電子メールがウイルスに感染されている場合、ユーザは、操作部２６を操作することにより、この電子メールを削除することができる（S204）。ユーザが削除操作をした場合は、メール記憶部２３から該当する電子メールが削除される（S205）。メール端末２０で行う他の処理は、さらに後述する。

【００５１】

図５は、表示部２４を介してユーザに表示される検査情報Ｍ１１の内容を示す説明図である。例えば、受信した電子メールがウイルスに感染していることを警告するメッセージを表示させることができる（Ｇ１）。また、ウイルスの種別（Ｇ２）や対処法（Ｇ３）を警告メッセージと併せて表示することもできる。さらに、携帯電話のような小型のメール端末２０の場合は、物理的サイズの制約上、表示部２４の表示面積が小さいため、全ての情報を一度に表示するのが難しい場合がある。その場合は、詳細な内容を階層化して表示するようにしてもよい（Ｇ４，Ｇ５）。あるいは、画面をスクロールさせることにより詳細な内容を閲覧するようにしてもよい。

【００５２】

ここで、対処法としては、「削除」を挙げることができる。「削除」とは、ウイルスに感染した電子メールの全体をメール記憶部２３から削除するものである。これに限らず、例えば、「全体削除」、「部分削除（添付ファイルのみ削除）」のように、より細分化された選択肢をユーザに提示してもよい。

【００５３】

一方、例えば、電子メールに感染しているウイルスの種類が古く、メール端末２０のコンピュータプログラムが既に対応済みであるような場合は、電子メールがウイルスに感染していても、ウイルスの発動による悪影響が発生しない。従って、この場合は「削除」せずに保存することができる。ウイルスの発動による悪影響が発生し得る場合であっても、ユーザが希望する場合は、電子メールを削除せずに保存することができる。この場合、電子メールは、通常の正常な電子メールと同様にメール記憶部２３内に保存される。但し、図６及び図７と共に後述するように、ウイルスに感染した電子メールの表示（添付プログラムの実行）及び転送には、制限がかけられているため、安全上の問題は生じない。

【００５４】

次に、図６のフローチャートは、メール端末２０内に保存された電子メールを表示させる場合の処理を示す。

【００５５】

電子メールの閲覧を希望するユーザーが操作部２６を介して所定の表示操作を行うと、本処理が開始される。操作部２６の操作に応じて、メール処理部２２は、メール記憶部２３内に記憶されている電子メールの中から該当する電子メールを参照し（S211）、この電子メールに付加されている検査情報Ｍ１１を検出してウイルス感染の判定結果を確認する（S212）。

【００５６】

電子メールがウイルスに感染していると判定された場合は（S213:YES）、判定結果を警告メッセージ等で表示すると共に、メール内容の表示を禁止する（S214）。つまり、表示部２４には、判定結果のみが表示される。ここで、禁止されるメールの内容には、電子メールに添付されたプログラムファイルが含まれており、ウイルス発動のおそれのある添付プログラムを実行させないように制御する。なお、ウイルスが添付ファイルにのみ存在し、メール本文の安全性が判明している場合は、添付されたプログラムファイルの実行のみを制限し、メール本文の閲覧は許可することもできる。

【００５７】

一方、ウイルスに感染していない電子メールの場合は（S213:NO）、電子メールの内容が全て表示され、添付されたプログラムファイルがある場合は、そのプログラムも実行される（S215）。

【００５８】

次に、図７のフローチャートは、メール端末２０に保存された電子メールを転送する場合の処理を示す。ここで「転送」とは、メールの差出人に「返信」する場合も含む。

【００５９】

メール端末２０のメール記憶部２３内に保存されている電子メールの転送を希望するユーザーが、操作部２６を介して所定の転送操作を行うと本処理が開始される。操作部２６の入力に応じて、メール処理部２２は、メール記憶部２３に記憶されている電子メールの中から該当する電子メールを参照する（S221）。

【００６０】

次に、参照された電子メールについて検査情報Ｍ１１が検出され、この検査情報Ｍ１１に基づいてウイルス感染の判定結果が確認される（S222）。転送しようとする電子メールがウイルスに感染している場合は（S223:YES）、判定結果を表示すると共に、メールの転送を禁止する（S224）。例えば、「このメールはウイルス＊＊＊に感染しているため、転送することができません。」等のメッセージを表示部２４に表示させることができる。一方、電子メールがウイルスに感染していない正常なメールである場合は（S223:NO）、ユーザが指定するアドレスに電子メールが転送される（S225）。

【００６１】

本実施の形態は上述の通りであって、これにより以下の効果を奏する。

【００６２】

メール端末２０内でウイルス感染の判定を行わず、メールサーバ１０側で行うため、ウイルス判定に関してメール端末２０側での処理負荷が発生しない。従って、ＣＰＵ処理能力や搭載メモリ量に制約を受ける携帯電話や携帯情報端末等の小型のメール端末の場合に特に有効である。

【００６３】

また、メールサーバ１０側で一元的にウイルス感染の判定を行うため、ウイルスパターンやウイルス検出プログラムの更新は、メールサーバ１０だけで行えばよく、ウイルス判定に関するメンテナンスを効率的に行うことができる。

【００６４】

メールサーバ１０側で予めウイルス感染の判定を行い、その判定結果を検査情報に含めて電子メールのヘッダに記述するため、ウイルス判定機能を備えないメール端末２０のユ

ーザにウイルス感染の有無を報知することができる。

【００６５】

また、検査情報にウイルスへの対処法を含めておくことにより、ウイルスへの適切な対処をユーザに促すことができると共に、コンピュータ知識の乏しいユーザに安心感を与えることができる。

【００６６】

さらに、ウイルスに感染している電子メールの表示や転送を禁止することにより、ウイルスの発動による悪影響や他の端末への二次感染を未然に防止することができる。

【００６７】

また、検査情報を電子メールのヘッダに記述するため、電子メールを受信したメール端末２０側では、メールの差出人や経路情報等の基本的なメール属性とウイルス判定に関する属性とを速やかかつ容易に検出することができる。

【実施例２】

【００６８】

次に、図８及び図９に基づいて、本発明の第２の実施の形態を説明する。なお、以下の説明では、上述した構成要素と同一の構成要素には同一の符号を付し、その説明を省略するものとする。本実施の形態の特徴は、ウイルスに感染した電子メールを調査する外部装置には、ウイルス感染の有無に関わりなく電子メールの転送を許可する点にある。

【００６９】

外部メール処理機器４０は、例えば、ウイルス検査プログラム等を搭載したパーソナルコンピュータや専用の装置等として構成されるもので、制御部４１，インターフェース（以下「Ｉ／Ｆ」）４２及びメール処理部４３を備えている。

【００７０】

外部メール処理機器４０は、Ｉ／Ｆ４２を介してメール端末２０のＩ／Ｆ２７に有線又は無線で接続されている。Ｉ／Ｆ２７，４２を介して取り込まれた電子メールは、メール処理部４３によって調査等される。制御部４１は、メール処理部４３やＩ／Ｆ４２の作動を制御する。

【００７１】

図９は、本実施の形態に係る転送処理のフローチャートを示す。本処理は、図６と共に述べた転送処理に、新規なステップＳ２３１及びＳ２３２を備えたものである。

【００７２】

ユーザが所定の操作を行うことにより電子メールの転送が指示された場合は、ユーザにより指定された転送先が外部メール処理機器４０であるか否かを判定する（S231）。そして、転送先が外部メール処理機器４０である場合は、ウイルス感染の有無を調べることなく、電子メールを外部メール処理機器４０に転送させる（S232）。

【００７３】

ここで、例えば、転送先として指定されたアドレスが「***@****.com」のように、ユーザ名＋ドメイン名で表現されており、他のメール端末へのメールアドレスである場合は、外部メール処理機器への転送と判断せずに転送を禁止することができる。あるいは、電子メールの転送に使用するＩ／Ｆの種類を検出することによって、電子メールの転送先が外部メール処理機器４０であるか否かを判定することもできる。さらには、例えば、外部メール処理機器４０からメール端末２０に、メール調査用の操作メニュープログラムを送信し、この調査用操作メニュープログラムから転送プログラムが呼び出された場合は、外部メール処理機器への転送であると判断することもできる。

【００７４】

ウイルスに感染している電子メールの詳細な調査を行う場合、メールサーバ１０を経由して返信すると二次感染の恐れがある。しかし、本実施の形態では、電子メールの転送先が、メール端末２０と直接的に接続されている外部メール処理機器４０である場合に、ウイルス判定結果の内容如何に関わらず転送を可とするため、ウイルスの二次感染拡大を阻止しながら、ウイルスの調査を行うことができる。

【００７５】
つまり、いわゆるローカル接続された端末（外部メール処理機器４０）には電子メールの転送を無条件で許可し、外部ネットワーク（インターネット３１）を介して接続される端末への転送は、ウイルス判定の結果に応じて許可されるようになっている。但し、安全性確保の点からは、メール端末２０とローカル接続された端末であっても、メール調査用のプログラム等のようなウイルス処理用のプログラムを備えていない場合には、転送を許可しないように構成することが好ましい。この場合、例えば、メール端末２０から外部メール処理機器４０に電子メールを転送する前に、外部メール処理機器４０がウイルス処理機能を有するか否かをメール端末２０から問合せ（あるいは、メール端末２０からの問合せを待たずに外部メール処理機器から自発的にウイルス処理機能の有無を宣言させることも可能）、S231において、「転送先は、ウイルス処理機能を有する外部機器か否か？」と判定すればよい。

【実施例３】

【００７６】
次に、図１０は、本発明の第３の実施の形態に係るメールサーバ側の処理を示すフローチャートである。本実施の形態の特徴は、ウイルスに感染した電子メールを部分的に削除してメール端末２０に配信する点にある。

【００７７】
電子メールがメールサーバ１０に到着すると（S111）、ウイルス判定が行われ（S112）、検査情報Ｍ１１が電子メールのヘッダに付加される（S113）。電子メールがウイルスに感染していない場合は（S114:NO）、電子メールがそのままメール記憶部１３に保存される（S115）。これに対し、電子メールがウイルスに感染している場合は（S114:YES）、電子メールからウイルス感染部分（あるいはウイルスに感染している危険性の高い部分）が削除され（S116）、ヘッダの情報と検査情報のみが（あるいは電子メール中の他の無害な部分と共に）メール記憶部１３に保存される（S117）。このようにして、保存された電子メールは、メール端末２０に配信される（S118）。

【００７８】
ここで、ウイルスに感染している電子メールの場合は、ヘッダ及び検査情報以外の全てを一律に削除して保存することもできるし（方法１）、ウイルスに感染している可能性の高い添付プログラムファイルのみを一律に削除して保存することもできるし（方法２）、さらには、電子メール中からウイルス感染部分のみを削除して保存することもできる（方法３）。

【００７９】
方法１及び方法２の場合は、電子メールの全体中から、予め設定された部分のみを一律に機械的に削除するため、処理内容が簡単であり、多量の電子メールを速やかに処理することができる。これに対し、方法３の場合は、各電子メール毎に個別の処理を行うため、処理内容が複雑化し、大量のメール処理には向かないが、ユーザに対して無害な部分をより多く提示できるため利便性が向上する。いずれの方法を採用してもよい。ユーザの希望に応じて、あるいは、電子メールの特性に応じて処理方法を選択することもできる。電子メールの特性に応じて処理する例を挙げると、例えば、同じメールアドレスから大量に発信された電子メールの場合は、方法１又は方法２を用いて処理し、それ以外の場合は方法３を用いることができる。

【００８０】
本実施の形態によれば、メールサーバ１０側でウイルスに感染していると判断された電子メールの内容の一部を削除するため、ウイルスに感染したと判断された電子メールをメール端末２０が受信しても、ウイルス発動による悪影響を低減することができ、より一層安全性が高まる。

【実施例４】

【００８１】
図１１は、本発明の第４の実施の形態に係る電子メールシステムの全体構成を示す説明

図である。本実施の形態の特徴は、図１中に示す無線基地局３２に代えて、インターネット３３を用い、このインターネット通信網３３を介してメールサーバ１０とメール端末５０とを接続している点にある。

【００８２】

メール端末５０は、第１の実施の形態で述べたメール端末２０と同様に、制御部５１，メール処理部５２，メール記憶部５３，表示部５４，報知部５５及び操作部５６を備えて構成することができる。

【００８３】

このようなメール端末５０としては、例えば、ファクシミリ装置、固定電話、インターネット接続機能を備えた各種電気製品（例えば、冷蔵庫、洗濯機、電子レンジ、音響製品、カーナビゲーションシステム、ＧＰＳ）等を挙げることができる。

【実施例５】

【００８４】

図１２及び図１３に基づいて、本発明の第５の実施の形態を説明する。本実施の形態の特徴は、ウイルスに感染した電子メールを受信したユーザには課金を行わない点にある。

【００８５】

即ち、メールサーバ１０には、各メール端末２０のユーザに対する課金を管理するための課金データベース１７が設けられており、この課金データベース１７の記憶内容に基づいて、各ユーザへの費用請求が行われる。

【００８６】

図１３は、メールサーバ１０の課金処理を示すフローチャートである。課金対象となっている電子メールのウイルス判定結果を確認し（S121）、課金対象の電子メールがウイルスに感染していないと判定された場合は（S122:NO）、通常通り、電子メールの受信者に所定の料金を課金する（S123）。これに対し、電子メールがウイルスに感染していると判定されていた場合は（S122:YES）、メール受信者への課金処理を中止する（S124）。そして、課金データベース１７を更新して処理を終了する（S125）。

【００８７】

これにより、ウイルスに感染した電子メールを送りつけられたユーザが課金されるのを防止して、顧客満足度を向上させることができる。

【実施例６】

【００８８】

図１４は、本発明の第６の実施の形態に係るメールサーバの課金処理を示すフローチャートである。本実施の形態の特徴は、ウイルスに感染していない正常な電子メールを受信したユーザには正規の料金を課金するが（S133）、ウイルスに感染している電子メールの場合は、受信者に課金せず、ウイルス感染メールの送信者に課金する（S134）点にある。

【００８９】

つまり、ウイルス感染メールの送信者が携帯電話を利用して電子メールを送信した場合、メールサーバ１０の課金データベース１７等を参照することにより、送信者を特定することができるので、ウイルス感染メールを発信したことについて送信者にペナルティを課すことができる。また、これに加えて、ウイルス感染メールの送信者に、ウイルスに感染した電子メールが送信された旨の注意を喚起する警告文を電子メールで自動的に返信するようにしてもよい。この警告の電子メールは、前記第５の実施の形態でも用いることができる。

【実施例７】

【００９０】

図１５及び図１６を参照して、本発明の第７の実施の形態を説明する。本実施の形態の特徴は、図２と共に述べたように、メールサーバ１０からメール端末２０に対して、検査情報Ｍ１１を含んだヘッダだけを先に送信し、ユーザの明示の指示を待ってから電子メールの全体を送信する点にある。

【００９１】

図１５は、メールサーバ側の処理を示す。電子メールが到着すると（S141:YES）、ウイルス判定が行われ（S142）、検査情報Ｍ１１を電子メールのヘッダ内に追記した後（S143）、メール記憶部１３に保存される（S144）。メール端末２０から電子メールの送信が要求されると（S145:YES）、このメール端末２０宛の電子メールがウイルスに感染しているか否かが判定される（S146）。

【００９２】

ウイルスに感染していない電子メールの場合は、電子メールの全体が直ちにメール端末２０に向けて送信される（S147）。これに対し、ウイルスに感染している電子メールの場合は（S146:YES）、電子メールのヘッダ（ヘッダには検査情報Ｍ１１が含まれている）のみが先にメール端末２０に送信される（S148）。

【００９３】

そして、ユーザからの指示を待ち（S149）、ユーザがウイルスに感染している電子メールの受信を希望する場合は、再度の確認をメール端末２０を介してユーザに行い（S150）、ユーザの受信意思が再確認された場合は（S150:YES）、ウイルスに感染している電子メールをメール端末２０に送信する（S147）。ユーザが電子メールの受信を取りやめた場合（S150:NO）及びユーザが電子メールの削除を希望する場合は、その電子メールをメール記憶部１３から削除する（S151）。

【００９４】

図１６は、メール端末側の処理を示す。電子メールの着信を検出すると（S241:YES）、メールサーバ１０から電子メールのヘッダのみが先に送信され（S242）、このヘッダ内に含まれている検査情報Ｍ１１に基づいて、ウイルス感染の判定結果がユーザに報知及び表示される（S243）。ユーザは、検査情報の表示内容に基づいて、電子メールの受信又は削除を選択することができる（S244）。電子メールの削除を選択した場合は、メールサーバ１０に対して該当する電子メールの削除を要求する（S245）。一方、電子メールの受信を希望する場合は、メールサーバ１０に対して電子メールの送信要求が行われ（S246）、これにより、メールサーバ１０から改めて送信されてきた電子メールの全体がメール記憶部２３に保存される（S247）。

【００９５】

このように構成される本実施の形態でも、前記第１の実施の形態と同様の効果を得ることができる。これに加えて、本実施の形態では、ウイルスに感染している電子メールの場合は、直ちに電子メール全体を送信するのではなく、検査情報を含んだヘッダのみを先に送信し、ユーザの明確な指示を待ってから電子メールを送信するため、より一層安全性を向上させることができる。

【００９６】

なお、本発明は、上述した各実施の形態に限定されない。当業者であれば、実施の形態で述べた構成に新たな構成要素を追加したり、削除したり、変更等したりして種々の変形を行うことができる。

【図面の簡単な説明】

【００９７】

【図１】本発明の第１の実施の形態に係る電子メールシステムの全体構成を示す説明図である。

【図２】電子メールの構成及び送信方法等を模式的に示す説明図である。

【図３】ヘッダ及びヘッダ内に追記される検査情報の記載内容を示す説明図である。

【図４】メールサーバ及びメール端末の処理の全体概要をそれぞれ示すフローチャートである。

【図５】ウイルスに感染した電子メールを受信した場合に、メール端末の表示部に表示される内容を示す説明図である。

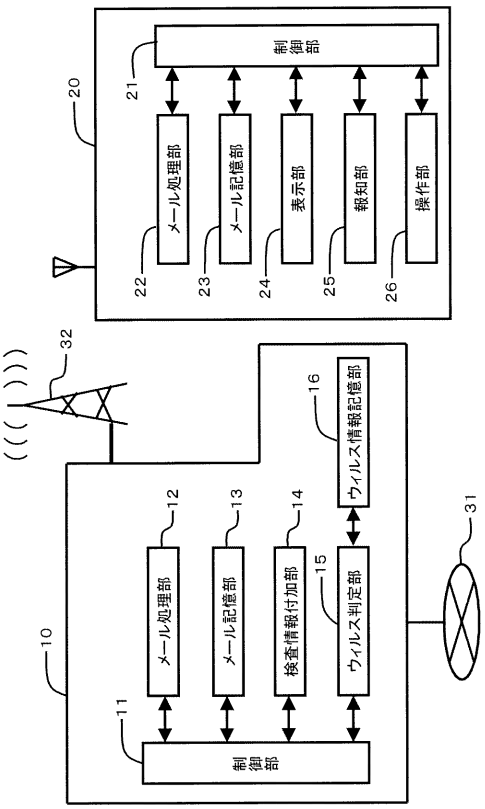
【図６】電子メールを表示させる場合の処理を示すフローチャートである。

【図７】電子メールを転送させる場合の処理を示すフローチャートである。

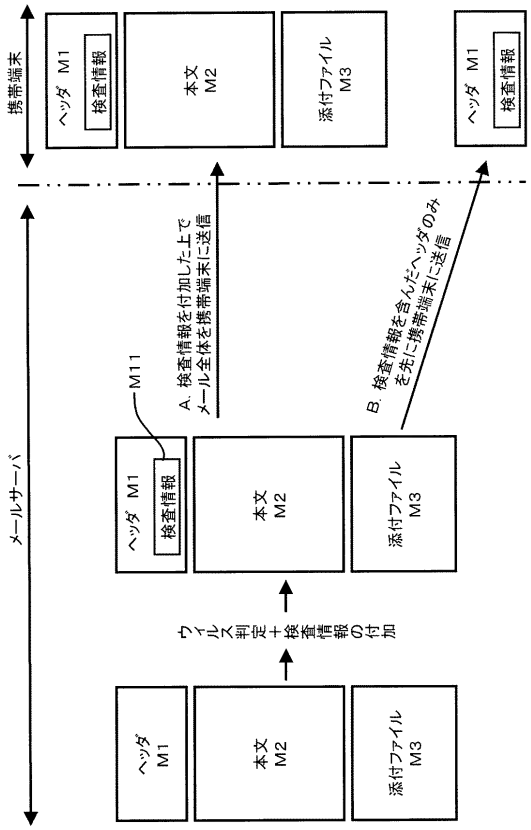
【図８】本発明の第２の実施の形態に係る電子メールシステムの要部を概略的に示す構成

説明図である。
【図９】メール転送処理を示すフローチャートである。
【図１０】本発明の第３の実施の形態に係るメールサーバの処理を示すフローチャートである。
【図１１】本発明の第４の実施の形態に係る電子メールシステムの全体概要を示す説明図である。
【図１２】本発明の第５の実施の形態に係る電子メールシステムの全体概要を示す説明図である。
【図１３】課金処理を示すフローチャートである。
【図１４】本発明の第６の実施の形態に係る電子メールシステムにおける課金処理を示すフローチャートである。
【図１５】本発明の第７の実施の形態に係る電子メールシステムにおけるメールサーバ側の処理を示すフローチャートである。
【図１６】メール端末側の処理を示すフローチャートである。
【符号の説明】
【００９８】
１０　メールサーバ
１１　制御部
１２　メール処理部
１３　メール記憶部
１４　検査情報付加部
１５　ウイルス判定部
１６　ウイルス情報記憶部
１７　課金データベース
２０　メール端末
２１　制御部
２２　メール処理部
２３　メール記憶部
２４　表示部
２５　報知部
２６　操作部
２７　通信Ｉ／Ｆ
３１　インターネット通信網
３２　無線通信基地局
３３　インターネット通信網
４０　外部メール処理機器
５０　メール端末

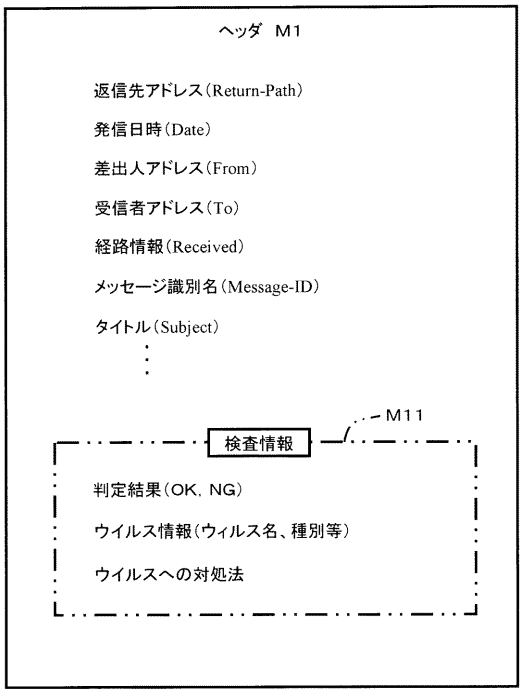
【図１】


制御部
メール処理部
メール記憶部
表示部
報知部
操作部
ウィルス情報記憶部
検査情報付加部
ウィルス判定部
制御部
10
11
12
13
14
15
16
20
21
22
23
24
25
26
31
32

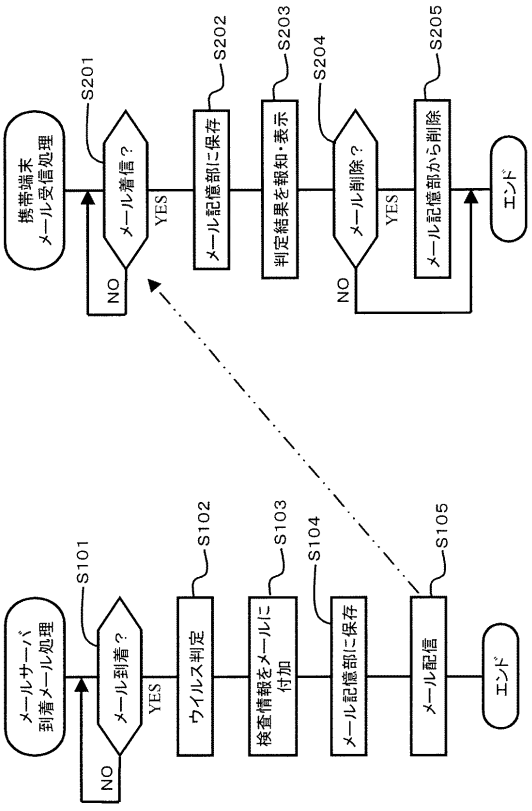
【図２】


携帯端末
ヘッダ M1
検査情報
本文 M2
添付ファイル M3
メールサーバ
M11
A. 検査情報を付加した上でメール全体を携帯端末に送信
B. 検査情報を含んだヘッダのみを先に携帯端末に送信
ウィルス判定＋検査情報の付加

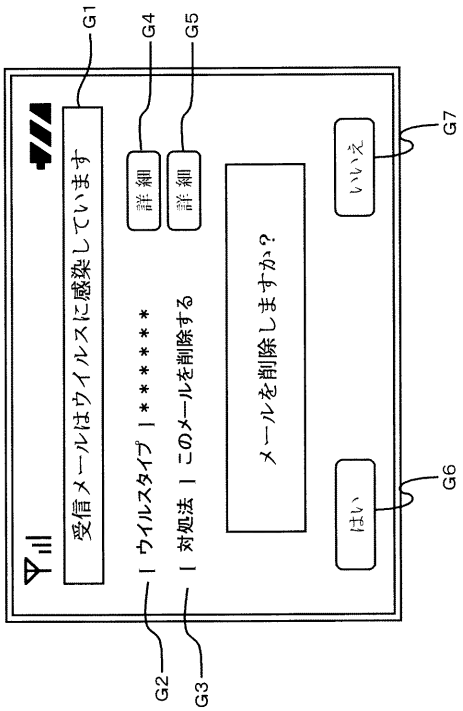
【図３】


ヘッダ M1
返信先アドレス(Return-Path)
発信日時(Date)
差出人アドレス(From)
受信者アドレス(To)
経路情報(Received)
メッセージ識別名(Message-ID)
タイトル(Subject)
検査情報
M11
判定結果(OK, NG)
ウイルス情報(ウィルス名、種別等)
ウイルスへの対処法

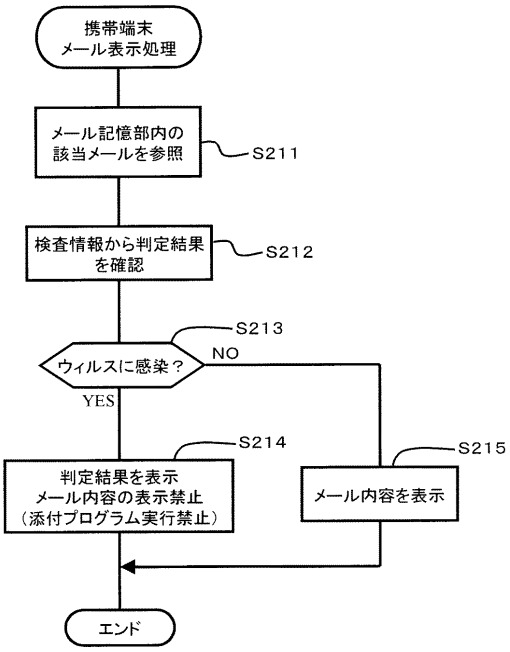
【図４】


携帯端末 メール受信処理
メール着信？
NO
YES
メール記憶部に保存
判定結果を報知・表示
メール削除？
NO
YES
メール記憶部から削除
エンド
S201
S202
S203
S204
S205
メールサーバ 到着メール処理
メール到着？
NO
YES
ウイルス判定
検査情報をメールに付加
メール記憶部に保存
メール配信
エンド
S101
S102
S103
S104
S105

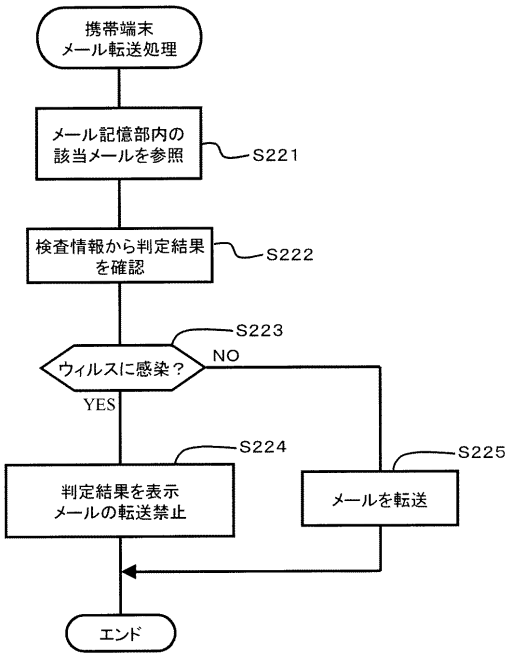
【図５】


G1
G4
G5
受信メールはウィルスに感染しています
詳細
詳細
ウィルスタイプ ｜＊＊＊＊＊＊
対処法 ｜ このメールを削除する
メールを削除しますか？
いいえ
はい
G7
G6
G2
G3

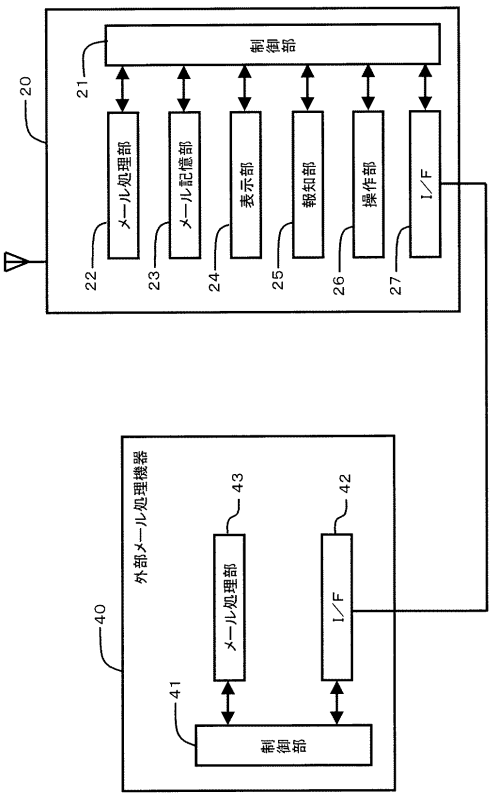
【図６】


携帯端末
メール表示処理
メール記憶部内の
該当メールを参照
S211
検査情報から判定結果
を確認
S212
S213
ウィルスに感染？
NO
YES
S214
判定結果を表示
メール内容の表示禁止
（添付プログラム実行禁止）
S215
メール内容を表示
エンド

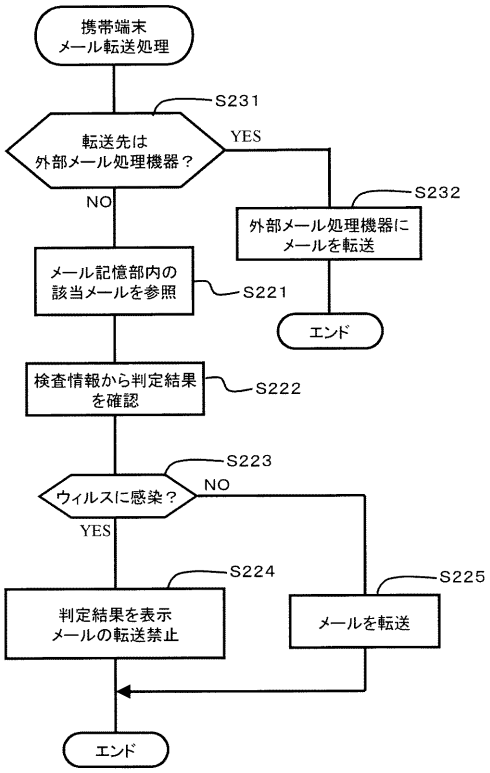
【図７】


携帯端末
メール転送処理
メール記憶部内の
該当メールを参照
S221
検査情報から判定結果
を確認
S222
S223
ウィルスに感染？
NO
YES
S224
判定結果を表示
メールの転送禁止
S225
メールを転送
エンド

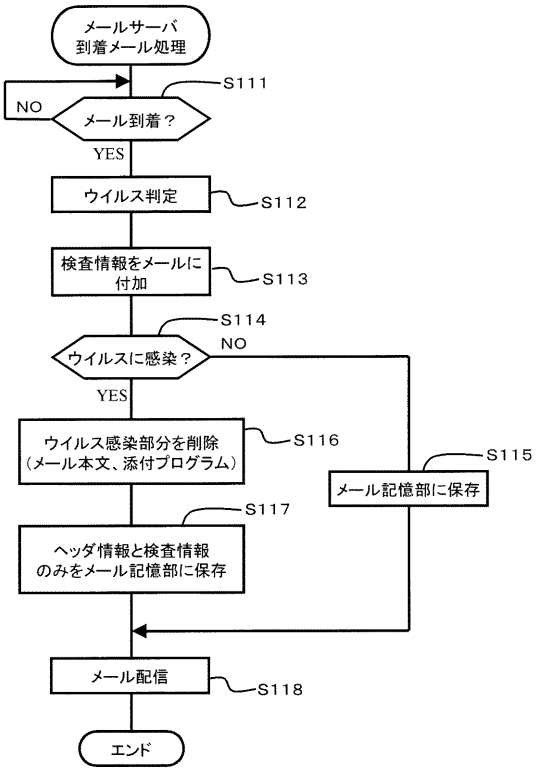
【図８】


制御部
21
20
メール処理部
メール記憶部
表示部
報知部
操作部
I／F
22
23
24
25
26
27
外部メール処理機器
43
42
メール処理部
I／F
40
41
制御部

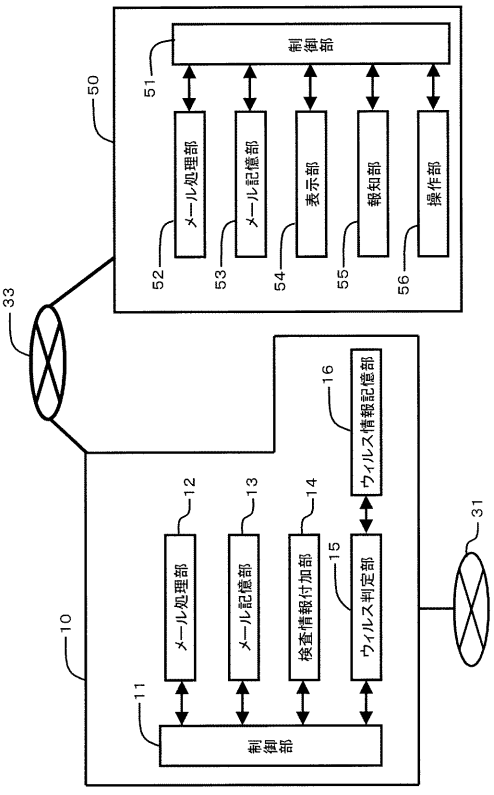
【図９】



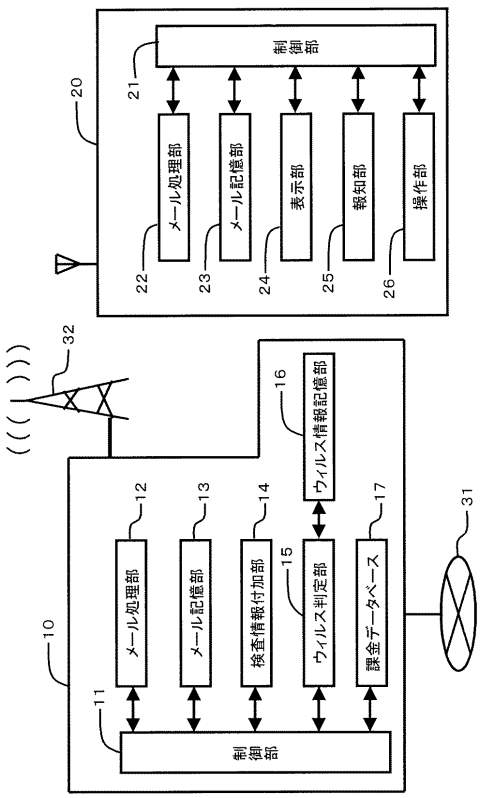
【図１０】



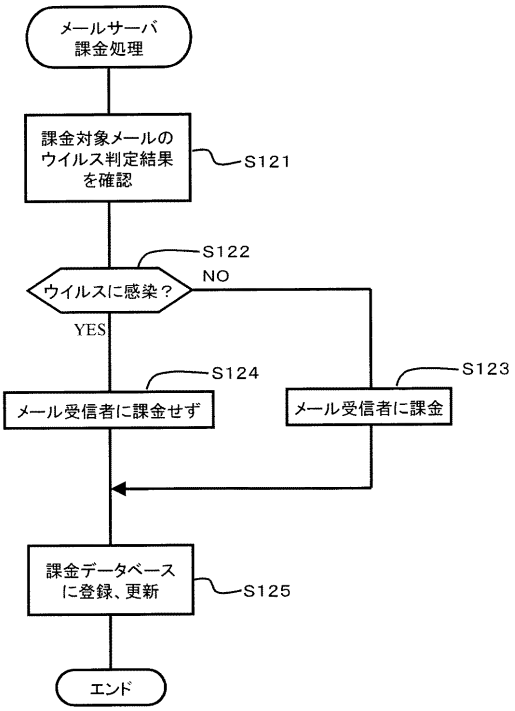
【図１１】



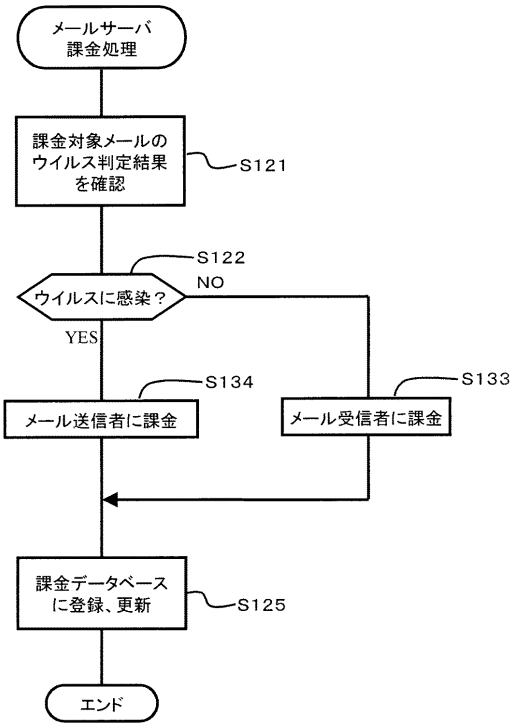
【図１２】



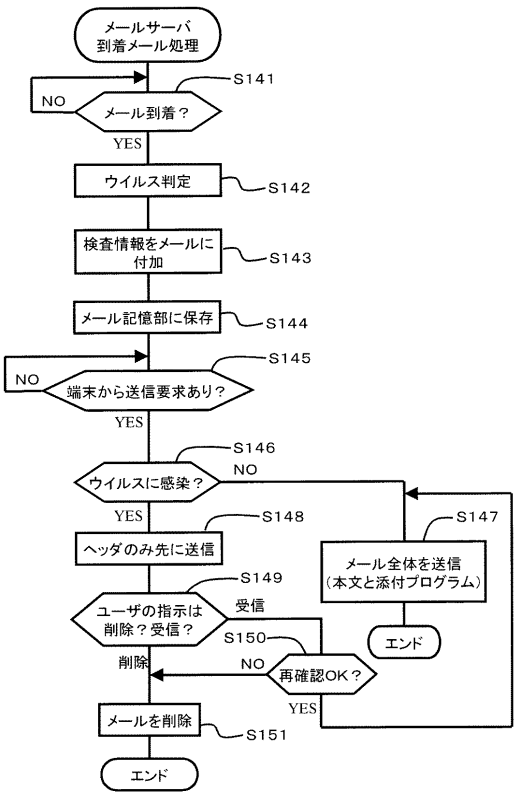
【図１３】



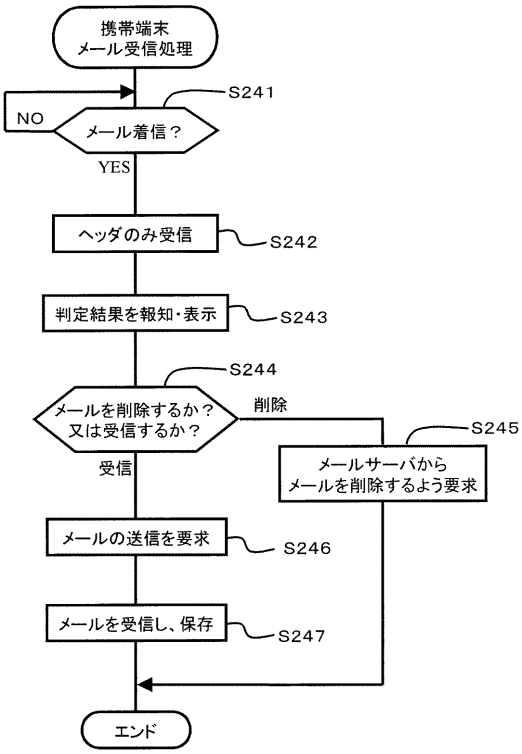
【図１４】



【図１５】



【図１６】



フロントページの続き

(72)発明者　長谷川　修
茨城県ひたちなか市稲田１４１０番地　株式会社日立製作所　デジタルメディア製品事業部内

審査官　清水　稔

(56)参考文献　西村　崇，ネット業者がウイルス対策に本腰、メールのウイルスを駆除するサービスを提供，日経コンピュータ，２０００年１０月２３日，第507号，p.40～42

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５８
Ｇ０６Ｆ　１３／００