(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-5436
(P2004-5436A)
(43)公開日　平成16年1月8日(2004.1.8)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 13/00	G06F	13/00	630A	5B076
G06F 11/00	H04L	12/58	100Z	5K030
H04L 12/58	G06F	9/06	660N	

審査請求 未請求　請求項の数 11　ＯＬ　（全 11 頁）

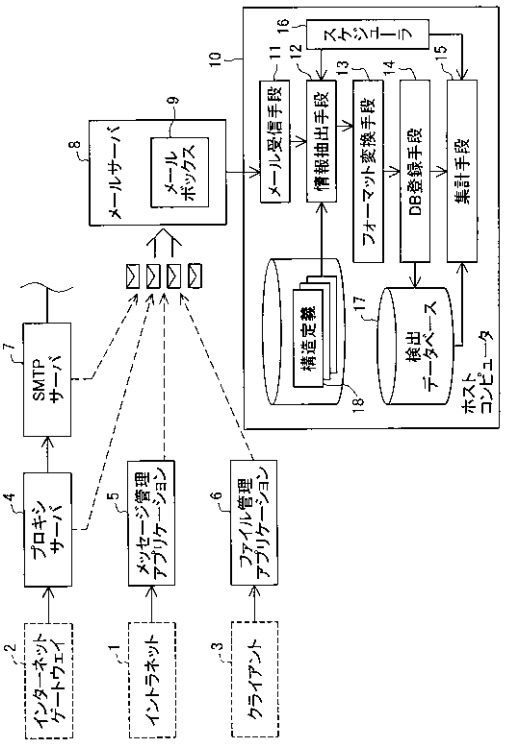
(21)出願番号　特願2003-37902(P2003-37902)
(22)出願日　平成15年2月17日(2003.2.17)
(31)優先権主張番号　特願2002-93139(P2002-93139)
(32)優先日　平成14年3月28日(2002.3.28)
(33)優先権主張国　日本国(JP)

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　110000028
特許業務法人明成国際特許事務所
(72)発明者　黒田　直人
長野県諏訪市大和三丁目３番５号　セイコーエプソン株式会社内

Ｆターム(参考)　5B076 FD08
5K030 GA15　HA05　KA07　MB15　MC07

(54)【発明の名称】電子メールを用いる情報収集システム

(57)【要約】
【課題】様々な書式で各種のアプリケーションから送信されるメールを自動的に解析し、その中から必要な情報を抽出して自動的にデータベースに登録する。
【解決手段】システムは、ウィルスに対する防御のために、システムの各部でウィルス駆除アプリケーションを動作させる。それぞれ独自に動作するウィルス駆除アプリケーションからは、随時その動作履歴等を含む情報がメールによりメールサーバ８に送信され、メールボックス９に収納される。構造定義１８は、メール中のデータベース作成に必要な情報の書き込まれた位置や書式を表示する。情報抽出手段１２は、構造定義１８を参照し、メール受信手段１１が受信したメールから必要な情報を抽出する。データベース登録手段１４は、その結果をデータベース１７に登録する。集計手段１５は、データベース１７から、例えば過去１ヶ月分のウィルス駆除情報を抽出して、報告書２５を得る。
【選択図】　図１



【特許請求の範囲】
【請求項１】
電子メールに基づいて所定の情報を収集する情報収集装置であって、
前記所定の情報を含む電子メールを読み込むメール読込部と、
前記電子メール中で前記所定の情報が記載してある箇所を特定するための構造定義を、前記電子メールの書式に応じて複数種類記憶する記憶部と、
前記電子メールの書式に基づいて前記構造定義を参照し、該電子メールから前記所定の情報を抽出する情報抽出部とを備える情報収集装置。
【請求項２】
請求項１記載の情報収集装置であって、
前記電子メールの書式は、該電子メールの送信者、宛先、タイトルの少なくとも一部を表す特定情報に対応付けて規定されており、
前記情報抽出部は、該特定情報に基づいて前記構造定義を参照する情報収集装置。
【請求項３】
請求項１記載の情報収集装置であって、
前記構造定義は、前記所定の情報の直前および直後に記載されるべき文字列の少なくとも一方を規定する情報収集装置。
【請求項４】
請求項１記載の情報収集装置であって、
前記構造定義は、前記電子メールの書式に基づいて適用可否を特定するための適用条件を含んでいる情報収集装置。
【請求項５】
請求項１記載の情報収集装置であって、
前記構造定義は、前記抽出された所定の情報を、その内容に応じて規定の文字列に変換するための変換規則を含んでおり、
前記情報抽出部は、該変換規則に基づいて、前記所定の情報の変換を行う情報収集装置。
【請求項６】
請求項１記載の情報収集装置であって、
前記記憶部は、前記複数種類の構造定義を、個別のファイルとして記憶する情報収集装置。
【請求項７】
請求項１記載の情報収集装置であって、
所定のタイミングで自動的に前記情報抽出部を起動する抽出制御部を備える情報収集装置。
【請求項８】
請求項１記載のメール情報収集システムにおいて、
前記抽出された所定の情報に基づき、所定の集計データを生成する集計部を備える情報収集装置。
【請求項９】
請求項８記載のメール情報収集システムにおいて、
前記所定の情報は、ウィルスの感染状況に関する情報であり、
前記集計データは、ウィルスに感染した感染ファイルの発信者ごとに、該感染ファイルの発信数を表しており、
前記集計部は、前記メール読込部による電子メールの読み込みをトリガとして、前記集計データの生成を行うメール情報収集システム。
【請求項１０】
電子メールに基づいて所定の情報を収集する情報収集方法であって、
前記所定の情報を含む電子メールを読み込む工程と、
前記電子メール中で前記所定の情報が記載してある箇所を特定するための構造定義を、前記電子メールの書式に応じて複数種類記憶する記憶部を予め準備する工程と、

前記電子メールの書式に基づいて前記構造定義を参照し、該電子メールから前記所定の情報を抽出する工程とを備える情報収集方法。
【請求項１１】
電子メールに基づいて所定の情報を収集するためのコンピュータプログラムであって、
前記所定の情報を含む電子メールを読み込む機能と、
前記電子メール中で前記所定の情報が記載してある箇所を特定するための構造
定義を、前記電子メールの書式に応じて複数種類記憶する記憶部を参照する機能と、
前記電子メールの書式に基づいて前記構造定義を参照し、該電子メールから前記所定の情報を抽出する機能とをコンピュータに実現させるためのコンピュータプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、電子メールを利用して所定の情報を収集するための情報収集システムに関する。
【０００２】
【従来の技術】
インターネットが普及し、ネットワークの利用度が高まるにつれて、コンピュータウィルスによる弊害が様々な分野に及ぶようになっている。ウィルスによる弊害を防止するために、ネットワークに接続された機器には、ウィルス駆除プログラムがインストールされている。ウィルス駆除プログラムは、例えば電子メールおよびその添付ファイルを検査し、ウィルスが検出されたファイルの削除、隔離などの処理を実行する。
【０００３】
ウィルス駆除プログラムには、ウィルス処理の結果を電子メールなどの形式で管理用サーバに報告する機能を備えるものがある。ネットワークの管理者は、管理用サーバに収集された電子メールの内容に基づいて、ウィルスの感染、駆除状況を把握することができる。
【０００４】
【特許文献１】
特開平９－２２４９６９号公報
【特許文献２】
特開平１１－１３６２７８号公報
【０００５】
【発明が解決しようとする課題】
通常、大規模なネットワークでは、ウィルス駆除プログラムは、各クライアント、サーバ、ゲートウェイなどの多くのデバイスにインストールされている。これらのウィルス駆除プログラムには統一がとれてない場合もあり、管理サーバに届けられる電子メールの書式がまちまちになることがあった。かかる場合には、ウィルス駆除に関する状況把握に要する管理者の負担が非常に大きかった。
【０００６】
かかる課題は、ウィルス駆除に関わらず、種々の書式からなる電子メールにより情報収集を行う際に共通の課題であった。本発明は以上の点に着目してなされたもので、様々な書式の電子メールを自動的に解析し、その中から必要な情報を自動的に抽出可能とすることを目的とする。
【０００７】
【課題を解決するための手段およびその作用・効果】
本発明では、以下の構成を有する情報収集装置によって、電子メールに基づいて所定の情報を収集する。本発明の情報収集装置は、電子メール中で収集対象となる所定の情報が記載してある箇所を特定するための情報（以下、「構造定義」と称する）を、電子メールの書式に応じて複数種類記憶する。そして、これらの情報を含む電子メールを読み込み、その書式に基づいて構造定義を参照して、所定の情報を抽出する。
【０００８】

このように、書式に応じて構造定義を使い分けることによって、種々の書式で送信された電子メールの内容を適切に解析でき、所望の情報を抽出することが可能となる。本発明の対象となる電子メールは、必ずしもアプリケーションが自動的に作成したものに限定はされず、人間が所定の書式に従って作成したものであってもよい。前者の例としては、例えば、ウィルス駆除アプリケーションによって作成される電子メールが含まれる。

【０００９】

構造定義の使い分けは、種々の方法で行うことができる。例えば、電子メールの書式が、電子メールの送信者、宛先、タイトルの少なくとも一部を表す特定情報に対応付けて規定されている場合には、これらの特定情報に基づいて構造定義を参照するものとしてもよい。通常、電子メールの送信者、宛先、タイトルは、電子メールの本文を解析するまでなく取得することが可能である。従って、これらを特定情報として用いることにより、迅速、的確に構造定義の使い分けを行うことができる。

【００１０】

一例として、電子メールがウィルス駆除プログラムなどのアプリケーションによって自動的に生成されるものである場合、書式はアプリケーションごとに異なることが多い。電子メールはアプリケーションがインストールされているクライアント等から発信されるため、結局、書式は電子メールの送信者と対応づけられることになる。電子メールの送信者を特定する情報、例えば、送信者アドレスは、このように、種々のアプリケーションが混在して利用される場合に、特定情報として有効活用できる。

【００１１】

別の例として、一つのクライアントに目的の異なる複数のアプリケーションがインストールされている場合を考える。各アプリケーションでは、目的に応じて種々の情報を含んだ電子メールが作成される。通常、これらの電子メールはタイトルが相違するため、電子メールの書式は、タイトルと関連づけられることになる。電子メールのタイトルは、このように、目的の異なるアプリケーションからの情報を処理する場合に、特定情報として有効活用できる。

【００１２】

本発明において、構造定義は、種々の形式で作成可能である。例えば、電子メールの本文の行数、カラム数で、情報の記載位置を特定する形式としてもよい。また、抽出対象となる所定の情報の直前および直後の少なくとも一方に記載されるべき文字列を用いて記載位置を特定する形式としてもよい。抽出対象となる情報には、見出しが付けられていることが多いため、これらの見出しを用いることにより、容易に記載位置を特定することができる。行数、カラム数などが異なる電子メールに対しても、これらの見出し等の文字列が一致している限り、共通の構造定義を流用することができる利点もある。

【００１３】

本発明において、構造定義には、情報の記載位置を特定する内容に加えて、種々の情報を含めることができる。例えば、電子メールの書式に基づいて適用可否を特定するための適用条件を構造定義に含めても良い。また、抽出された所定の情報を、その内容に応じて規定の文字列に変換するための変換規則を含めてもよい。これらの情報を構造定義に含めることにより、情報収集装置自体の処理内容を改変しなくても構造定義の追加、変更に対応することが可能となる。例えば、情報収集装置には、構造定義に含まれる適用条件と電子メールの書式を対比する汎用的な機能を備えておけば、構造定義の使い分けを実現することができる。

【００１４】

本発明では、複数種類の構造定義を、個別のファイルとして記憶することが好ましい。こうすることにより、対象となる電子メールの種類、書式の変動に比較的容易に対応することが可能となる。

【００１５】

構造定義は、種々の言語で作成することが可能であるが、柔軟性に富むという意味で、ＸＭＬなどのマークアップ言語を用いることが好ましい。マークアップ言語を用いた構造定

義では、タグによって、先に説明した適用条件、変換規則などを含めることも比較的容易に実現可能である。

【００１６】

本発明において、情報の抽出は、オペレータの操作に基づいて行うものとしてもよいが、所定のタイミングで自動的に情報抽出部を起動可能とすることが好ましい。こうすることにより、オペレータの負荷を更に軽減することができる。タイミングは、例えば、一日単位というように時間的な基準で設定してもよいし、未処理の電子メール数やデータ量の基準で設定してもよい。

【００１７】

本発明において、抽出された情報は、種々の態様で活用することができる。例えば、抽出された情報に基づいて所定の集計データを生成するようにしてもよい。抽出された情報を、一旦、データベースに蓄積した後、集計データの生成を行うようにしてもよい。かかる集計処理は、オペレータの操作に基づいて行うものとしてもよいし、所定のタイミングで自動的に行うようにしてもよい。例えば、予め設定された一定周期で行うものとしてもよいし、一定量のデータが蓄積された時点で行うものとしてもよい。また、電子メールの読み込みをトリガとするイベントドリブンで集計データの生成を行うものとしてもよい。

【００１８】

集計データの内容は種々の設定が可能である。例えば、ウィルスの感染状況に関する情報を含む電子メールを取り扱う場合には、ウィルスに感染した感染ファイルの発信者ごとに、感染ファイルの発信数を表す集計データを生成してもよい。かかる集計データは、ウィルスの感染源となっているデバイスの特定に有効活用することができる。特に、コンピュータに備えられているアドレス帳に掲載された各メールアドレスに対して、ウィルスに感染した電子メールを自動的に配信するタイプのウィルスへの対策に有用である。このような利用方法においては、対策の迅速化のため、上述したイベントドリブンで集計データの生成を行うことが好ましい。

【００１９】

抽出された情報、または集計された結果は、ネットワークを介して予め設定された配信先に配信してもよいし、Ｗｅｂページなどの形式で各利用者が閲覧可能としてもよい。

【００２０】

本発明は上述の情報収集装置としての構成に限らず、情報収集方法として構成してもよい。情報収集をコンピュータに行わせるためのコンピュータプログラム、またはかかるコンピュータプログラムを記録したコンピュータ読取可能な記録媒体として構成してもよい。ここで、記録媒体としては、フレキシブルディスクやＣＤ－ＲＯＭ、光磁気ディスク、ＩＣカード、ＲＯＭカートリッジ、パンチカード、バーコードなどの符号が印刷された印刷物、コンピュータの内部記憶装置（ＲＡＭやＲＯＭなどのメモリ）および外部記憶装置等、コンピュータが読取り可能な種々の媒体を利用できる。

【００２１】

【発明の実施の形態】

以下、本発明の実施の形態を実施例に基づき説明する。

Ａ．システム構成

Ｂ．構造定義

Ｃ．情報抽出処理

Ｄ．集計例

Ｅ．効果

Ｆ．変形例

【００２２】

Ａ．システム構成

図１は実施例としての情報収集システムの構成を示す説明図である。情報収集システムは、電子メールを利用して、ネットワーク上の種々のコンピュータ、デバイスからウィルスに関する情報を収集するためのシステムである。本実施例のシステムは、メールサーバ８

とホストコンピュータ１０で構成される。

【００２３】

本実施例において、ウィルス情報に関する電子メールは、各デバイス等にインストールされたウィルス駆除アプリケーションによって送信される。図には、ウィルス駆除アプリケーションがインストールされるデバイス等を例示した。かかるデバイスとしては、例えば、企業内のイントラネット１からインターネットに接続するためのインターネットゲートウェイ２に接続されたプロキシサーバ４や、ＳＭＴＰサーバ７が挙げられる。イントラネット１に接続された管理用のコンピュータで稼働するメッセージ管理アプリケーション５も含まれる。イントラネット１に接続されるクライアント３で稼働するファイル管理アプリケーション６も含まれる。メールサーバ８には、それぞれのウィルス駆除アプリケーションがウィルスを検出すると、ウィルス情報を含む電子メールが送信される。これらの電子メールは、メールボックス９に収納され、ホストコンピュータ１０によって周期的に処理される。

【００２４】

ホストコンピュータ１０は、電子メールに含まれた情報の解析を行う。図中には、ホストコンピュータ１０の機能ブロックを併せて示した。本実施例では、ホストコンピュータ１０に情報解析用のソフトウェアをインストールすることにより、これらの機能ブロックが構築される。各機能ブロックは、ハードウェア的に構成することも可能である。

【００２５】

メール受信手段１１は、メールボックス９から解析対象となる電子メールを取得する。情報抽出手段１２は、電子メールの内容を解析し、ウィルスに関する情報を抽出する。この解析には、予め用意された構造定義１８が用いられる。構造定義１８とは、電子メールに、どのような形式でウィルスに関する情報が含まれているかを定義する情報である。構造定義１８の内容については、後で詳述する。構造定義１８は、ホストコンピュータ１０内部に記憶しておいてもよいし、ＣＤ－ＲＯＭなどの記録媒体やネットワークを介して外部から読み込むようにしてもよい。

【００２６】

フォーマット変換手段１３は、情報抽出手段１２によって抽出された情報を、データベースに一括して登録するためにフォーマット変換する。適用可能なフォーマットとしては、例えば、ＣＳＶ形式、即ちカンマで区切りつつ、所定の項目順にデータを並べた形式が挙げられる。

【００２７】

データベース登録手段１４は、フォーマット変換されたウィルス情報を、検出データベース１７と称するデータベースに登録する。集計手段１５は、検出データベース１７のデータに基づいて、種々の統計処理を行って、過去１ヶ月分のウィルス駆除情報などの報告書を作成する。ホストコンピュータ１０の管理者は、この報告書を、印刷したり、ネットワークを介して配信したりすることで、ウィルスの活動情報を各利用者に知らせることができる。

【００２８】

スケジューラ１６は、予め設定されたタイミングで、周期的に電子メールの解析や報告書の作成を行わせる機能を奏する。スケジューラ１６は、カレンダー情報を内蔵しており、例えば１日１回とか、午前と午後に１回ずつなど予め設定されたスケジュールで、情報抽出手段１２を稼働させる。同様に、例えば１週間に１回、１ヶ月に１回など予め設定されたスケジュールで、集計手段１５を稼働させる。情報抽出手段１２と集計手段１５の稼働は、同一のスケジュールで行っても良いし、個別に設定可能としてもよい。スケジュールは、上述した一定周期という設定だけでなく、メールボックス９や検出データベース１７における未処理の情報が所定量に達した時点などの設定を用いてもよい。

【００２９】

Ｂ．構造定義

図２は構造定義の例を示す説明図である。図３はウィルス情報を含む電子メール例を示す

説明図である。構造定義および電子メールには、説明の便宜上、左側に行番号を付した。電子メールには、１行目の「ウィルス検知報告」のように、統計上、不要なコメント文が含まれている。構造定義は、このような電子メール中で、有用なウィルス情報が記載されている場所を規定する文書である。本実施例では、構造定義はＸＭＬで記載した。

【００３０】

図２に示す例において、８～１２行目は、構造定義を適用するための条件を既定している。この例では、９行目に示す「ウィルス検知報告」、１０行目に示す「インターネットメールゲートウェイ」というコメントが電子メール中に見いだされることが一つめの条件となる。１１行目では、電子メール中で「受信者」と「発信者」の間に記載されている文字列中に、ドメイン名「ｅｐｓｏｎ．ｃｏ．」が含まれることを規定している。図３の電子メール例では、７行目において、ウィルスが含まれたファイルの受信者を表す文字列、「ｒｅｃｉｐｉｅｎｔ@ｅｐｓｏｎ．ｃｏ．ｊｐ」が、上述のドメイン名を含むことが条件となる。つまり、この構造定義は、上述のドメインに属する者宛のファイルから検出されたウィルス情報の処理に適用されることになる。

【００３１】

構造定義（図２）の１３～２５行目では、情報の抽出方法およびコード変換の方法を規定する。１４行目では、「ＳｍｔｐＧＷ」と「Ｄａｔｅ」で囲まれた文字列、即ち、ウィルス情報を送信したデバイス（図３の電子メールの４行目）「ＳＭＴＰ」を抽出することを規定している。同様にして、１５～１９行目で、ウィルスを含むファイルの受信者、ウィルスを含むファイルの送信者、ウィルス名、感染ファイル名、ウィルスの処理という各情報について抽出方法を規定している。図３の電子メールでは、この定義に基づき、７～１２行目の情報がそれぞれ抽出される。

【００３２】

２０～２４行目では、ウィルスの処理について、コードに変換する方法を規定している。この例では、「ｒｅｊｅｃｔ」処理はコード「１」、「ｍｏｖｅ」処理はコード「３」、その他の処理はコード「８」に変換される。

【００３３】

構造定義は、図２の例示に限らず、種々の構成を採ることができる。抽出すべき情報も任意に設定可能である。例えば、ウィルス駆除の日時などの情報を取得してもよい。本実施例では、ＸＭＬを用いて構造定義を記述したが、任意の言語を使用可能である。

【００３４】

ウィルス情報を含む電子メールの書式は、ウィルス駆除アプリケーションによって異なる。本実施例では、かかる相違に対応するため、ウィルス駆除アプリケーションごとに構造定義を用意しておくものとした。ウィルス情報を含む電子メールは、ウィルス駆除アプリケーションによって発信されるから、この電子メールの送信元アドレスによって、構造定義を使い分けることができる。本実施例では、構造定義の使い分けを判断する情報として、適用可能な送信元アドレスのリストを各構造定義に対応づけて管理する。送信元アドレス毎に個別に構造定義を管理するようにしてもよい。構造定義は、ネットワークのいずれかのデバイスに新規なウィルス駆除プログラムがインストールされるたびに、追加登録される。

【００３５】

Ｃ．情報抽出処理

図４は電子メール解析処理のフローチャートである。スケジューラ１６が、予め設定されたタイミングでトリガを発生することにより、開始される処理である。

【００３６】

ホストコンピュータ１０は、予め用意された構造定義１８およびメールボックス９の未読の電子メールを読み出す（ステップＳ２、Ｓ３）。次に、電子メールの送信元アドレスに該当する構造定義を読み出す。構造定義が存在しない場合には、エラー処理を行う（ステップＳ１０）。

【００３７】

構造定義が存在する場合には、ホストコンピュータ１０は、この構造定義に基づいて電子メールから集計の対象となる情報を抽出する（ステップＳ５）。そして、抽出された情報のフォーマットを変換し（ステップＳ６）、検出データベース１７に登録する（ステップＳ７）。フォーマット変換を省略し、抽出された情報を直接、検出データベース１７のレコードとして追記する方法を採ってもよい。

【００３８】

これらの処理が完了すると、ホストコンピュータ１０は、情報の抽出が完了した電子メール、およびエラーとなった電子メールを、共に予め設定されたフォルダに保管する（ステップＳ８）。例えば、送信元別などで用意されたサブフォルダに分類して保管するものとしてもよい。ホストコンピュータ１０は、以上の処理を、メールボックス９の全ての未読メールについて繰り返し実行する（ステップＳ９）。

【００３９】

Ｄ．集計例

図５はウィルス駆除記録の出力例を示す説明図である。図１に示した集計手段１５が出力する報告書の一例である。タイトルに示した名称（×××．ｗｒｓ）というウィルスの駆除記録を示した。駆除記録では、駆除したウィルスの件数が、駆除日別に棒グラフによって示さる。棒グラフは、事業所別に出力される。「前月ボタン」前月の駆除記録が表示される。「処理別リスト」ボタンをクリックすると、各ウィルスに施された処置の記録が表示される。「ウィルス種別リスト」ボタンをクリックすると、一月中に駆除されたウィルスの種類および件数が表示される。

【００４０】

図６はウィルス種別リストの出力例を示す説明図である。このリストでは、駆除件数が多い順にウィルスが表示される。駆除件数は、グラフ表示される。図５、図６は、出力例に過ぎず、報告書の形式、表示項目などは種々の態様を採ることができる。

【００４１】

Ｅ．効果

本実施例のシステムによれば、ウィルス駆除アプリケーションが作成した電子メールからウィルス情報を自動的に抽出して、データベースに登録することができる。構造定義を使い分けることにより、書式の異なる電子メールが混在している場合でも、適切に情報の抽出を行うことができる。この結果、ネットワーク上のウィルス情報の管理・解析にかかる人的負荷を軽減することができる。

【００４２】

Ｆ．変形例

電子メールの解析およびデータの集計は、種々のタイミングで行うことが可能である。例えば、ウィルス駆除アプリケーションが作成した電子メールの受信をトリガとして処理を実行してもよい。

【００４３】

図７は変形例としての電子メール解析処理のフローチャートである。ウィルスに感染した電子メールの発信者の特定に有用な集計データの生成処理を例示した。この処理は、ウィルス駆除アプリケーションが作成した電子メールの受信をトリガとして、ホストコンピュータ１０がイベントドリブンで実行する処理である。

【００４４】

まず、ホストコンピュータ１０は、構造定義、未読メールおよび集計データの読み込みを行う（ステップＳ２０）。集計データとは、従前の処理で得られた結果を意味する。

【００４５】

受信した電子メールの解析に適した構造定義が存在しない場合には（ステップＳ２１）、実施例と同様、エラー処理を行い（ステップＳ２５）、メールを保管して（ステップＳ２６）、処理を終了する。

【００４６】

構造定義が存在する場合には（ステップＳ２１）、電子メールを解析して集計情報を抽出

する（ステップＳ２２）。この結果に基づいて、集計データを更新し（ステップＳ２３）、集計データの出力を行う（ステップＳ２４）。

【００４７】

図中に、集計データの出力例を示した。ウィルスに感染した電子メールの発信数をユーザごとに集計した結果を、グラフ出力する例である。かかる集計データを出力するための処理としては、ステップＳ２２で図２、図３で示した発信者情報を集計情報として抽出し、ステップＳ２３で、この発信者情報に該当するユーザの発信数を逐次増加させればよい。

【００４８】

ホストコンピュータ１０は、解析が終了した電子メールを保管し（ステップＳ２６）、処理を終了する。ここでは、ウィルスに感染した電子メールの発信数をユーザごとに集計する場合を例示したが、企業外から受信するメールについては、メールアドレスごとに集計してもよいし、メールアドレスに含まれるドメインごとに集計してもよい。

【００４９】

変形例の集計データは、例えば、クライアントに備えられているアドレス帳に掲載された各メールアドレスに対して、ウィルスに感染した電子メールを自動的に配信するタイプのウィルスへの対策に有用である。かかる集計データは、ウィルスの感染源を特定するのに有効活用することができる。変形例では、イベントドリブンで処理を実行するため、集計データのリアルタイム性を向上することができ、ウィルスへの迅速な対処が可能となる利点もある。

【００５０】

本実施例において、電子メールは、必ずしもウィルス駆除アプリケーションが自動的に発信するものには限定されない。所定の形式で担当者がマニュアルで作成した電子メールを解析対象とすることもできる。本実施例においては、データベースから報告書を作成する機能は省略しても差し支えない。本実施例は、ウィルス情報を含む電子メールに限らず、種々の電子メールを対象とすることができる。異なる目的を持ったアプリケーションによって生成された電子メールが混在してもよい。かかる場合には、例えば、送信者アドレスに限らず、電子メールのタイトルに基づいて構造定義を使い分けるようにしてもよい。

【００５１】

なお、各図に示した各機能ブロックは、それぞれ別々のプログラムモジュールにより構成してもよいし、一体化したプログラムモジュールにより構成してもよい。また、これらの機能ブロックの全部または一部を論理回路によるハードウエアで構成しても構わない。また、各プログラムモジュールは、既存のアプリケーションプログラムに組み込んで動作させてもよいし、独立のプログラムとして動作させてもよい。上記のような本発明を実現するためのコンピュータプログラムは、例えばＣＤ－ＲＯＭのようなコンピュータで読み取り可能な記録媒体に記録して、インストールして利用することができる。また、ネットワークを通じてコンピュータのメモリ中にダウンロードして利用することもできる。

【図面の簡単な説明】

【図１】実施例としての情報収集システムの構成を示す説明図である。

【図２】構造定義の例を示す説明図である。

【図３】ウィルス情報を含む電子メール例を示す説明図である。

【図４】電子メール解析処理のフローチャートである。

【図５】ウィルス駆除記録の出力例を示す説明図である。

【図６】ウィルス種別リストの出力例を示す説明図である。

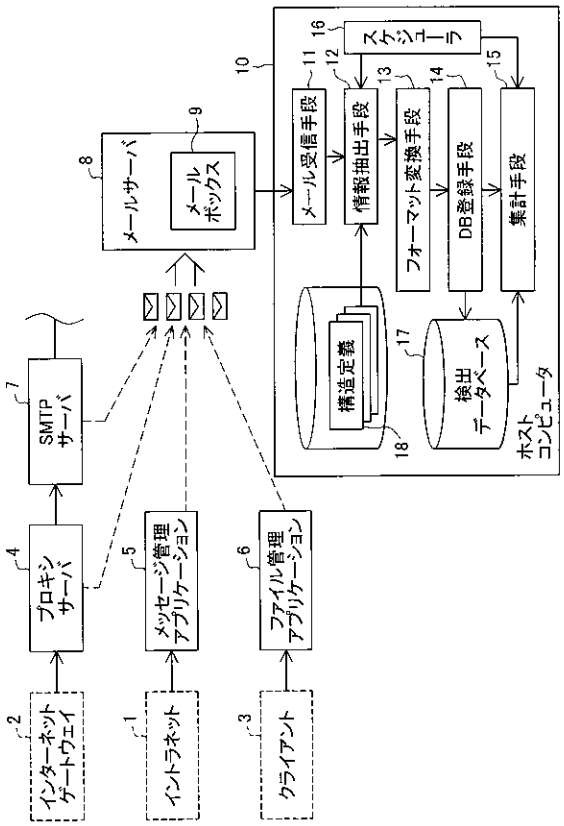
【図７】変形例としての電子メール解析処理のフローチャートである。

【符号の説明】

１…イントラネット
２…インターネットゲートウェイ
３…クライアント
４…プロキシサーバ
５…メッセージ管理アプリケーション

６…ファイル管理アプリケーション
７…ＳＭＴＰサーバ
８…メールサーバ
９…メールボックス
１０…ホストコンピュータ
１１…メール受信手段
１２…情報抽出手段
１３…フォーマット変換手段
１４…データベース登録手段
１５…集計手段
１６…スケジューラ
１７…検出データベース
１８…構造定義

【図１】



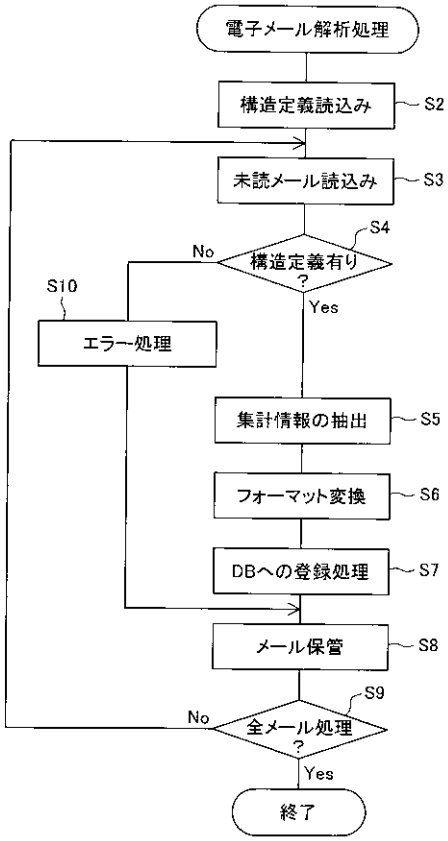
【図２】

```
<?xml version="1.0" encoding="Shift_JIS" ?>
<def>
<description>SMTP-Receive</description>
<virus_alert/>
<vaccine_type>4</vaccine_type>
<layer>1</layer>
<MoveFolder>Virusアラート¥SMTP-RECEIVE</MoveFolder>
<condition>
<entity>!! ウィルス検知報告 !!</entity>
<entity>インターネットメールゲートウェイ</entity>
<entity>受信者.*?epson¥.co.*?発信者</entity>
</condition>
<extract>
<SenderPC>SMTP GW : [dmt]Date</SenderPC>
<VirusDestination>受信者 :[dmt]発信者</VirusDestination>
<VirusSender>発信者:[dmt]ウィルス名</VirusSender>
<VirusName>ウィルス名:[dmt]感染ファイル名</VirusName>
<VirusAttached>感染ファイル名:[dmt]処理</VirusAttached>
<VaccineAction>処理:[dmt]詳細は</VaccineAction>
<convert>
<VaccineAction>reject[dmt]1</VaccineAction>
<VaccineAction>move[dmt]3</VaccineAction>
<VaccineAction><other/>[dmt]8</VaccineAction>
</convert>
</extract>
</def>
```

【図３】

```
1  "***** !! ウィルス検知報告 !! *****
2  インターネットメールゲートウェイにてウィルスが検知されました。
3
4  SmtpGW: SMTP
5  Date: 01/14/2003 14:54:50
6
7  受信者: recipient@epson.co.jp
8  発信者: infector@epson.co.jp
9
10 ウィルス名: VIRUS
11 感染ファイル名: 1.exe
12 処理: quarantined
```

【図４】



【図５】

ウィルス[×××.wrs]駆除記録

月	日	―― ××事業所 ---- ××事業所 ―・― ××研究所
8	1	
8	2	
8	3	
8	31	

ウィルス種別リスト　処置別リスト　前月

【図６】

ウィルス種別リスト

順位	ウィルス名	駆除件数
1位	×××.wrs	
2位	×××.××	
3位	×××××	
4位	×××××	

【図７】