(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2007-281702
(P2007-281702A)
(43)公開日　平成19年10月25日(2007.10.25)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 12/58	(2006.01)	H04L 12/58	100F	5K030

審査請求 未請求　請求項の数 21　ＯＬ　（全 15 頁）

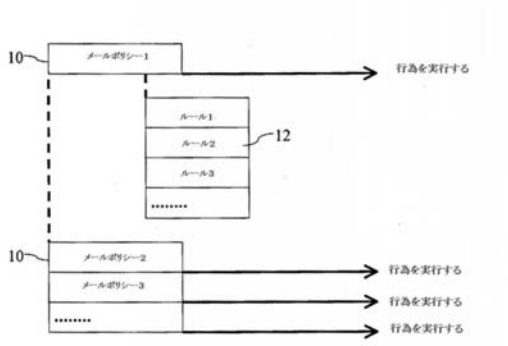
(21)出願番号　特願2006-103408 (P2006-103408)
(22)出願日　平成18年4月4日 (2006.4.4)

(71)出願人　505340294
碩▲き▼科技股▲ふん▼有限公司
台灣新竹縣竹北市縣政路５８號４樓
(74)代理人　100080252
弁理士　鈴木　征四郎
(72)発明者　鄭志文
台湾新竹縣竹北市縣政六路５８號４樓

Ｆターム(参考)　5K030 GA15　HA06　KA07　LC15　LD11

(54)【発明の名称】電子メールの管理、制御方法

(57)【要約】
【課題】　電子メールの通信効率を低下させることなく、電子メールの管理と制御を正確に行うとともに、スパムメールを確実にブロックする電子メールの管理、制御方法を提供する。
【解決手段】　この発明の電子メールの管理、制御方法は、電子メールのエンベロープデータと、ヘッダーのデータを利用して、複数の異なるメールポリシーを予め設定するステップと、エージェント（Ａｇｅｎｔ）によって、受信する電子メールの伝送データを該複数の異なるメールポリシーに基づいて逐一照合して該電子メールの行為が該複数の異なるメールポリシーに該当するか否か認証し、かつ認証の結果に基づいて該電子メールのブロック／伝送する行為を行うステップとを含む。
【選択図】　図１



【特許請求の範囲】
【請求項１】
メールのエンベロープデータと、ヘッダーのデータを利用して、複数の異なるメールポリシーを予め設定するステップと、
エージェント（Ａｇｅｎｔ）によって、受信する電子メールの伝送データを該複数の異なるメールポリシーに基づいて逐一照合して該電子メールの行為が該複数の異なるメールポリシーに該当するか否か認証し、かつ認証の結果に基づいて該電子メールのブロック／伝送する行為を行うステップとを含むこと、を特徴とする電子メールの管理、制御方法。
【請求項２】
前記メールポリシーが、認証する電子メールがスパムメールであるか否かの判断を行うものであって、該エージェントが受信した電子メールを認証する方法が、受信した電子メールの送信データが該メールポリシーに該当するか否か逐一照合するステップと、照合の結果該メールポリシーに該当する場合に該電子メールがスパムメールであるとしてブロックするステップと、照合の結果該メールポリシーに該当しない場合に該電子メールを伝送するステップとを含むことを特徴とする請求項１に記載の電子メールの管理、制御方法。
【請求項３】
前記メールポリシーが電子メールの送受信を管理するポリシーであって、かつチェック不要のメール行為を設定するものであって、該エージェントが受信した電子メールを認証する方法が、受信した電子メールの受信データが該メールポリシーに該当するか否か照合するステップと、照合の結果該メールポリシーに該当する場合は該電子メールをチェック不要扱いの電子メールとして伝送するステップと、照合の結果該メールポリシーに該当しない場合は該電子メールをブロックするステップと、を含むことを特徴とする請求項１に記載の電子メールの管理、制御方法。
【請求項４】
前記チェック不要扱いとする電子メールの送信者が、本社、子会社、重要な顧客、取引のあるメーカー、講読するメールマガジンを提供するドメインネームもしくは固定ＩＰなどからなるグループの内の少なくとも１つであることを特徴とする請求項３に記載の電子メールの管理、制御方法。
【請求項５】
前記メールポリシーを設定するステップが、それぞれのメールポリシーの認証のルールを設定を含み、かつ該ルールが符合する、符合しない、もしくは照合することなく無視する内の一から選択されること
を特徴とする請求項１に記載の電子メールの管理、制御方法。
【請求項６】
前記電子メールの送信データが、該電子メールに属するエンベロープデータ及びヘッダーデータを含むことを特徴とする請求項１に記載の電子メールの管理、制御方法。
【請求項７】
前記受信した電子メールの送信データが該メールポリシーに該当するスパムメールであるか認証する方法が、次に掲げる（ａ）、（ｂ）、（ｃ）のステップを含み、
（ａ）のステップにおいて、該エージェントが受信した電子メールを第１のメールポリシーに従って該電子メールの送信データの真偽性を認証し、第１のメールポリシーに符合するか否か判断し、符合するのであれば（ｂ）のステップに進み、符合しない場合は（ｃ）のステップへ進み、
（ｂ）のステップにおいて、該電子メールの送信を許可し、
（ｃ）のステップにおいて、第２のメールポリシーに従い、継続して該電子メールのルートを遡って照合し第２のメールポリシーに符合するか否か判断し、符合すると判断した場合は（ｂ）のステップに進み、符合しないと判断した場合は次のメールポリシーに従って該電子メールのルートを遡って認証を行い、最後のメールポリシーに至まで継続して行い、かつ最後のメールポリシーに至るまで負メールポリシーに符合しない場合は、該電子メールをブロックすることを特徴とする請求項２に記載の電子メールの管理、制御方法。

【請求項８】
前記複数の異なるメールポリシーのそれぞれが複数のルールを含み、これらメールポリシーに従って受信した電子メールのデータに対して行う認証が次に掲げる（ａ）、（ｂ）、（ｃ）のステップを含み、
（ａ）のステップにおいて、第１のルールに従って電子メールの送信データについて、真偽を認証し、第１のルールに符合するか否か判断し、符合するのであれば（ｂ）のステップに進み、符合しない場合は（ｃ）のステップへ進み、
（ｂ）のステップにおいて、第２のルールに従い、継続して該電子メールの送信データの真偽を認証し、第２のルールに符合するか否か判断し、符合するのであれば（ｃ）のステップに進み、符合しないのであれば、次のルールに従って該電子メールのルートを遡って認証を行い、最後のルールに至るまで継続して行い、最後のルールによる認証結果に基づいて、該電子メールがメールポリシーに符合するか否か決定し、符合するのであれば該電子メールの伝送を許可して送信し、符合しない場合は（ｃ）のステップに進み、
（ｃ）のステップにおいて、次のメールポリシー内の規則に従い、該電子メールのルートを継続して遡り、メールポリシーに符合するか否か判断し、かつ該（ａ）、もしくは（ｂ）のステップを繰り返し行うことを特徴とする請求項２に記載の電子メールの管理、制御方法。
【請求項９】
前記複数のルールが、符合する、符合しない、もしくは照合することなく無視するの内の一から選択され、かつこれらルールがメールポリシーを設定するステップにおいて設定されることを特徴とする請求項８に記載の電子メールの管理、制御方法。
【請求項１０】
前記メールポリシーが、受信した電子メールが通常と異なる行為によるものか否か判断を行うものであって、通常と異なる行為が匿名、偽称、乱発、または非合法などの行為からなるグループの内の少なくとも一であることを特徴とする請求項１に記載の電子メールの管理、制御方法。
【請求項１１】
前記匿名の行為が、ヘッダのデータが不明瞭であるか、送信者のコンピュータと返信の宛先のコンピュータとが異なるか、または返信の宛先のコンピュータがインターネットサーバープロバイダのコンピュータであるといった行為からなるグループの内の少なくとも一を含むことを特徴とする請求項１０に記載の電子メールの管理、制御方法。
【請求項１２】
前記偽称の行為が、送信元のコンピュータが外部のドメインにありながら、送信者のアドレスを該ドメイン内のコンピュータのものであると偽称するか、もしくはドメインのドメインネームサーバが不正確であるなどの行為の内の一を含むことを特徴とする請求項１０に記載の電子メールの管理、制御方法。
【請求項１３】
前記乱発する行為が、送信方法が異常で、且つ頻繁に変動することを含むことを特徴とする請求項１０に記載の電子メールの管理、制御方法。
【請求項１４】
前記非合法方の行為が、返信するアドレスがレンタルしたコンピュータのものであることを含むことを特徴とする請求項１０に記載の電子メールの管理、制御方法。
【請求項１５】
前記メールポリシーが、電子メールの内容及び添付ファイルに従ってポリシーの内容を設定することを特徴とする請求項１に記載の電子メールの管理、制御方法。
【請求項１６】
前記エージェントが、メールトランスファエージェント（ＭＴＡ）であることを特徴とする請求項１に記載するメール行為の解析を利用した電子メールの管理、調整方法。
【請求項１７】
前記メールトランスファエージェント（ＭＴＡ）がルータであることを特徴とする請求項

１６に記載の電子メールの管理、制御方法。
【請求項１８】
前記エンベロープのデータが、送信者のアカウント、受信者のアカウント、受信者のアドレス、送信者のアドレス、返信アドレス、ドメインネーム、及びタイムスタンプからなるグループから選択されることを特徴とする請求項１６に記載の電子メールの管理、制御方法。
【請求項１９】
前記タイムスタンプが、送信サーバー、ＤＳＬＡＭ（Digital Subscriber Line Access Multiplexer）、もしくはインターネットサービスプロバイダ（ＩＳＰ）のサーバーからなるグループの内の少なくとも一から提供されることを特徴とする請求項１６に記載の電子メールの管理、制御方法。
【請求項２０】
前記電子メールをブロックする行為が、該電子メールの受信を拒絶するか、該電子メールを削除する処理方法から選択されることを特徴とする請求項１６に記載の電子メールの管理、制御方法。
【請求項２１】
前記電子メールの受信を拒否する処理方法が、同時にエラーコードと、エラーメッセージとを返信することを含むことを特徴とする請求項２０に記載の電子メールの管理、制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、電子メールの管理、制御方法に関し、特に電子メールを送受信するメール行為を分析して行う電子メールの管理・制御方法に関する。
【背景技術】
【０００２】
企業が電子メールを利用して情報を得ようとする場合、例えば、ウィルス、ハッカー等から、スパムメールの猖獗に至るまで多くの問題が存在する。これら問題の内スパムメールについては、電子メールの検査、ウィルス対策ソフトの提供、スパムメールのブロックを行うソフトの提供、及びこれらソフトのアップデートを提供する情報セキュリティサービスの会社は、そのほとんどがデータベースに保存した膨大なデータに基づき、これらデータに演算と分析の技術を加え、スパムメールに係る情報を収集し、更にデータの統計、分析などの計算を行い、人工知能を啓発してスパムメールをブロックする効果を達成している。
【０００３】
しかしながら、従来の技術は分類の認定が主観的過ぎるという点が欠点として挙げられる。即ちアダルト、財テク、薬物、ビジネスなどの分類が主観的で、決定性に欠け、誤った判断をする可能性があるとともに、メール内容のスキャナにコストを費やし、通信効率が下がる場合がある。
【０００４】
スパムメールをブロックするために、各国では相次いで関連する法令を制定している。国際的な共通の認識によれば、電子メールはスパムメールと広告用のメールに区分される。よってスパムメールのブロックを論じる前に、スパムメールと広告用のメールとの区別について論じなければならない。アメリカ合衆国を例に挙げると、アメリカ合衆国では、Ｃａｎ－Ｓｐａｍ法を制定し、匿名、偽称、無差別、もしくは非合法（変動データもしくはシークレットデータなど）の電子メールをスパムメールとしている。スパムメールがこれら行為による原因は、おそらく次の通りである。
１．　送信者を追求できない。
２．　連絡方法が変動的である。
３．　受信者が同僚、友人からのものであると誤認する。

４．受信者に好奇心を抱かせてメールを読ませる。
【０００５】
受信した電子メールの送信者が不明な場合、または受信を拒絶することができない場合、特殊な技術によって認識し、受信を拒絶しなければならない。
【０００６】
広告用の電子メールとは、送信者が特定のルートによって受信者のアドレスを取得し、正常に公開された方式で送信される電子メールを指す。受信者は送信者を追及することができ、且つ正式なルートで講読を取り消す権利を有する。
【０００７】
従来のスパムメールをブロックする技術は、大きく分けると内容のフィルタリング、数値の計算、及び啓発の３種類に分けられる。内容をフィルタリングする方法は、送信者、受信者、電子メールのヘッダ、電子メールの内容、拡張子、ファイル名、メールの本文などをフィルタリングしてブロックする。即ち、ブラックリストを収集してスパムメールをブロックする方法である。係る方法は、リストの収集が容易でない、リストの作成に時間がかかる、ブロックの成功率が高くない、ブラックリストからの判断に誤りが発生しやすいなどの欠点を有する。
【０００８】
数値計算の方法は、膨大なデータの演算と分析技術に基づいて迷惑メールの「メール内容」を大量に収集し、加算する方法によりスパムメール防止を達成する。しかし、かかる方法は分類（ポルノ、財テク、薬物、ビジネスなど）が主観的で、決定性がなく、誤った判断をする可能性があるとともに、メール内容のスキャナは費用がかかり、かつ通信効率を低下させるなどの欠点がある。技術啓発の方法は、前述の数値計算の方法と類似している。膨大なデータの演算と分析でスパムメールの「メール内容」を大量に収集し、メール内容を加算すると同時に、知的啓発方法を加える。よって、数値計算方法の欠点以外に、データが大きすぎる場合、誤判率が高くなる。
【発明の開示】
【発明が解決しようとする課題】
【０００９】
この発明は、電子メールの通信効率を低下させることなく、電子メールの管理と制御を正確に行うとともに、スパムメールを確実にブロックする電子メールの管理、制御方法を提供することを課題とする。
【課題を解決するための手段】
【００１０】
そこで、本発明の発明者は従来の技術に見られる欠点に鑑みて鋭意研究を重ねた結果、メールのエンベロープデータと、ヘッダーのデータを利用して、複数の異なるメールポリシーを予め設定するステップと、エージェント（Ａｇｅｎｔ）によって、受信する電子メールの伝送データを該複数の異なるメールポリシーに基づいて逐一照合して該電子メールの行為が該複数の異なるメールポリシーに該当するか否か認証し、かつ認証の結果に基づいて該電子メールのブロック／伝送する行為を行うステップとを含むこと電子メールの管理、制御方法によって課題を解決できる点に着眼し、かかる知見に基づいて本発明を完成させた。
【００１１】
以下、この発明について具体的に説明する。
請求項１に記載する電子メールの管理、制御方法は、メールのエンベロープデータと、ヘッダーのデータを利用して、複数の異なるメールポリシーを予め設定するステップと、エージェント（Ａｇｅｎｔ）によって、受信する電子メールの伝送データを該複数の異なるメールポリシーに基づいて逐一照合して該電子メールの行為が該複数の異なるメールポリシーに該当するか否か認証し、かつ認証の結果に基づいて該電子メールのブロック／伝送する行為を行うステップとを含む。
【００１２】

請求項２に記載する電子メールの管理、制御方法は、請求項１におけるメールポリシーが、認証する電子メールがスパムメールであるか否かの判断を行うものであって、該エージェントが受信した電子メールを認証する方法が、受信した電子メールの送信データが該メールポリシーに該当するか否か逐一照合するステップと、照合の結果該メールポリシーに該当する場合に該電子メールがスパムメールであるとしてブロックするステップと、照合の結果該メールポリシーに該当しない場合に該電子メールを伝送するステップとを含む。

【００１３】

請求項３に記載する記載の電子メールの管理、制御方法は、請求項１におけるメールポリシーが電子メールの送受信を管理するポリシーであって、かつチェック不要のメール行為を設定するものであって、該エージェントが受信した電子メールを認証する方法が、受信した電子メールの受信データが該メールポリシーに該当するか否か照合するステップと、照合の結果該メールポリシーに該当する場合は該電子メールをチェック不要扱いの電子メールとして伝送するステップと、照合の結果該メールポリシーに該当しない場合は該電子メールをブロックするステップと、を含む。

【００１４】

請求項４に記載する電子メールの管理、制御方法は、請求項１におけるチェック不要扱いとする電子メールの送信者が、本社、子会社、重要な顧客、取引のあるメーカー、講読するメールマガジンを提供するドメインネームもしくは固定ＩＰなどからなるグループの内の少なくとも１つである。

【００１５】

請求項５に記載する電子メールの管理、制御方法は、請求項１におけるメールポリシーを設定するステップが、それぞれのメールポリシーの認証のルール設定を含み、かつ該ルールが符合する、符合しない、もしくは照合することなく無視する、の内の一から選択される。

【００１６】

請求項６に記載する電子メールの管理、制御方法は、請求項１における電子メールの送信データが、該電子メールに属するエンベロープデータ及びヘッダーデータを含む。

【００１７】

請求項７に記載に記載する電子メールの管理、制御方法は、求項２における受信した電子メールの送信データが該メールポリシーに該当するスパムメールであるか認証する方法が、次に掲げる（ａ）、（ｂ）、（ｃ）のステップを含み、

（ａ）のステップにおいて、該エージェントが受信した電子メールを第１のメールポリシーに従って該電子メールの送信データの真偽性を認証し、第１のメールポリシーに符合するか否か判断し、符合するのであれば（ｂ）のステップに進み、符合しない場合は（ｃ）のステップへ進み、

（ｂ）のステップにおいて、該電子メールの送信を許可し、

（ｃ）のステップにおいて、第２のメールポリシーに従い、継続して該電子メールのルートを遡って照合し第２のメールポリシーに符合するか否か判断し、符合すると判断した場合は（ｂ）のステップに進み、符合しないと判断した場合は次のメールポリシーに従って該電子メールのルートを遡って認証を行い、最後のメールポリシーに至まで継続して行い、かつ最後のメールポリシーに至るまで負メールポリシーに符合しない場合は、該電子メールをブロックすること。

【００１８】

請求項８に記載する電子メールの管理、制御方法は、請求項２における複数の異なるメールポリシーのそれぞれが複数のルールを含み、これらメールポリシーに従って受信した電子メールのデータに対して行う認証が次に掲げる（ａ）、（ｂ）、（ｃ）のステップを含み、

（ａ）のステップにおいて、第１のルールに従って電子メールの送信データについて、真偽を認証し、第１のルールに符合するか否か判断し、符合するのであれば（ｂ）のステップに進み、符合しない場合は（ｃ）のステップへ進み、

（ｂ）のステップにおいて、第２のルールに従い、継続して該電子メールの送信データの真偽を認証し、第２のルールに符合するか否か判断し、符合するのであれば（ｃ）のステップに進み、符合しないのであれば、次のルールに従って該電子メールのルートを遡って認証を行い、最後のルールに至るまで継続して行い、最後のルールによる認証結果に基づいて、該電子メールがメールポリシーに符合するか否か決定し、符合するのであれば該電子メールの伝送を許可して送信し、符合しない場合は（ｃ）のステップに進み、
（ｃ）のステップにおいて、次のメールポリシー内の規則に従い、該電子メールのルートを継続して遡り、メールポリシーに符合するか否か判断し、かつ該（ａ）、もしくは（ｂ）のステップを繰り返し行う。

【００１９】

請求項９に記載する電子メールの管理、制御方法は、請求項８における複数のルールが、符合する、符合しない、もしくは照合することなく無視する、内の一から選択され、かつこれらルールがメールポリシーを設定するステップにおいて設定される。

【００２０】

請求項１０に記載する電子メールの管理、制御方法は、請求項１におけるメールポリシーが、受信した電子メールが通常と異なる行為によるものか否か判断を行うものであって、通常と異なる行為が匿名、偽称、乱発、または非合法などの行為からなるグループの内の少なくとも一である。

【００２１】

請求項１１に記載する電子メールの管理、制御方法は、請求項１０における匿名の行為が、ヘッダのデータが不明瞭であるか、送信者のコンピュータと返信の宛先のコンピュータとが異なるか、または返信の宛先のコンピュータがインターネットサーバープロバイダのコンピュータであるといった行為からなるグループの内の少なくとも一を含む。

【００２２】

請求項１２に記載する電子メールの管理、制御方法は、請求項１０における偽称の行為が、送信元のコンピュータが外部のドメインにありながら、送信者のアドレスを該ドメイン内のコンピュータのものであると偽称するか、もしくはドメインのドメインネームサーバが不正確であるなどの行為の内の一を含む。

【００２３】

請求項１３に記載する電子メールの管理、制御方法は、請求項１０における乱発する行為が、送信方法が異常で、且つ頻繁に変動することを含む。

【００２４】

請求項１４に記載する電子メールの管理、制御方法は、請求項１０における非合法方の行為が、返信するアドレスがレンタルしたコンピュータのものであることを含む。

【００２５】

請求項１５に記載する電子メールの管理、制御方法は、請求項１におけるメールポリシーが、電子メールの内容及び添付ファイルに従ってポリシーの内容を設定する。

【００２６】

請求項１６に記載する電子メールの管理、制御方法は、請求項１におけるエージェントが、メールトランスファエージェント（ＭＴＡ）である。

【００２７】

請求項１７に記載する電子メールの管理、調整方法は、請求項１６におけるメールトランスファエージェント（ＭＴＡ）がルータである。

【００２８】

請求項１８に記載する電子メールの管理、制御方法は、請求項１６におけるエンベロープのデータが、送信者のアカウント、受信者のアカウント、受信者のアドレス、送信者のアドレス、返信アドレス、ドメインネーム、及びタイムスタンプからなるグループから選択される。

【００２９】

請求項１９に記載する電子メールの管理、制御方法は、請求項１６におけるタイムスタン

プが、送信サーバー、ＤＳＬＡＭ（Digital Subscriber Line Access Multiplexer）、もしくはインターネットサービスプロバイダ（ＩＳＰ）のサーバーからなるグループの内の少なくとも一から提供される。

【００３０】

請求項２０に記載する電子メールの管理、制御方法は、請求項１６における電子メールをブロックする行為が、該電子メールの受信を拒絶するか、該電子メールを削除する処理方法から選択される。

【００３１】

請求項２１に記載する電子メールの管理、制御方法は、請求項２０における電子メールの受信を拒否する処理方法が、同時にエラーコードと、エラーメッセージとを返信することを含む。

【発明の効果】

【００３２】

この発明による電子メールの管理、制御方法は、電子メールの管理と制御を正確に行うとともに、スパムメールを効率よくブロックできるとともに、ネットワークの安全性を高め、ネットワークの帯域と、システムのリソースと、ハードディスクの空間とを節約して電子メールの通信効率を高め、運営コストを低減させるといった利点を有する。

【発明を実施するための最良の形態】

【００３３】

この発明は、メール集配信サーバー（Ｍａｉｌ　ｔｒａｎｓｆｅｒ　ａｇｅｎｔ、以下ＭＴＡと称する）が電子メールの処理を実行する段階において、予め設定されたメールポリシーに基づいて、電子メールのメール送信データの真偽値を認証し、エンベロープ、電子メールのヘッダなどの送信データを分析することによって、該電子メールの行為がシステムの許容する行為に適ったものか能動的に判断し、電子メールの送受信の管理、制御及びスパムメールをブロックするという目的を達成する。

【００３４】

１通の完全な電子メールをメールテキスト（Ｍａｉｌ　ｔｅｘｔ）と称する。一般にメールテキストは、メールエンベロープ（Ｍａｉｌ　ｅｎｖｅｌｏｐ）、メールヘッダ（Ｍａｉｌ　ｈｅａｄｅｒ）、メールコンテンツ（Ｍａｉｌ　ｃｏｎｔｅｎｔ）を含む。また、１通の完全な電子メールは、サーバーとクライアント端において、メール集配信サーバー、メールユーザーエージェント（Ｍａｉｌ　ｕｓｅｒ　ａｇｅｎｔ、ＭＵＡ）によって処理される。かかる過程は、電子メールの基本的な送信モードである。この発明は、係る電子メールの特性と送信の原則を利用し、電子メールのエンベロープ、ヘッダなどのメール伝送データの真偽値について分析を行い、且つリターンを繰り返して認証し、百種類を超えるメール行為のタイプを正確に帰納、演繹し、電子メール送受信の管理、制御及びスパムメールをブロックする作用を達成する

【００３５】

この発明は、電子メールのエンベロープデータに基づいて設定され、メールを管理するメールポリシーを利用する。よって、本発明の方法を説明する前に、エンベロープデータの内容について説明しなければならない。電子メールのエンベロープデータは、通常送信者のアカウント、受信者のアカウント、受信者のアドレス、送信者のアドレス、返信アドレス、ドメインネーム（Ｄｏｍａｉｎ　Ｎａｍｉｎｇ　Ｓｅｒｖｅｒ、ＤＮＳ）、及びタイムスタンプなどを含む。また、電子メールは送信サーバー、ＤＳＬＡＭ（Digital Subscriber Line Access Multiplexer）、もしくはインターネットサービスプロバイダ（ＩＳＰ）のサーバーなどのエージェントを経て送信され、それぞれのエージェントを通過する毎に電子メールにタイムスタンプを付与する。

【００３６】

図１は、本発明における電子メールを分析する行為、及び電子メールの管理、制御方法を示した説明図である。図面によれば、先ず電子メールのエンベロープデータ、ヘッダデータ、コンテンツ、及び添付ファイルなどのデータに基づいて、予め複数の異なる電子メー

ルポリシー１０を設定する。それぞれの電子メールポリシー１０は、複数のルール１２を含む。

【００３７】

図２に開示するように、それぞれの電子メールポリシー１０の設定は「送信者」、「受信者」、「メールヘッダ」の３種類のルールＬ１２を含む。３種類のルール１２の設定は、同時に符合しなければならない。同時に符合して始めてシステムが実行できる。ルール１２の設定について、ユーザーは符合する、符合しない、もしくは照合をスキップする、を指定することができる。即ち、ユーザーは電子メールの送信者、もしくは電子メールの受信者を指定することができ、記入しない場合は、いずれをも有することを表す。また、メールヘッダーを照合するか、照合をスキップするか選択することができる。全てのルール１２の間における関連性はアンドであって、これら設定の全てに符合して始めて条件が成立したものと見なされ、システムが適宜な行為を実行する。同様に電子メールポリシー１０を設定する場合、必要に応じて符合する、符合しない、及び照合をスキップする、の内の一つを指定することができる。

【００３８】

電子メールポリシー１０、及びそのルール１２を設定した後、エージェントが電子メールを受け取ると、これら電子メールポリシー１０に基づき、電子メールのメール送信データに対して逐一照合を行う。照合するメール送信データは、該電子メールに属するエンベロープ、ヘッダデータを含み、時にはコンテンツ、及び添付ファイルを含む場合もある。これらは予め設定された電子メールポリシー１０、及びそのルール１２によって決まる。該電子メールの行為がこれら電子メールポリシー１０に符合するか否かを認証し、認証の結果に基づき対応するブロック／送信の動作を行う。

【００３９】

電子メールポリシー１０、及びそのルール１２は、これらを設定する者によってスパムメールの行為か、もしくは検査不要メールの行為として設定することができ、これをもって電子メールがスパムメールであるか否かを判断するか、もしくは電子メールがチェック不要の扱いを受けるメールであるか否かを判断する。電子メールポリシー１０、及びそのルール１２がスパムメールの行為として定義された場合、エージェントが電子メールを受け取り、該電子メールを認証する場合、電子メールポリシー１０に基づき、該電子メールのメール送信データについて逐一照合を行って、該電子メールの行為が、電子メールポリシー１０に符合するか、認証する。認証するのであれば、該電子メールがスパムメールであるということを表し、該電子メールをブロックする。符合しない場合は、該電子メールを送信する。

【００４０】

逆に、電子メールポリシー１０、及びそのルール１２がチェック不要メールの行為として設定されている場合、エージェントは電子メールを受信した後、電子メールポリシー１０に従って、該電子メールのメール送信データについて照合を行い、該電子メールの行為が電子メールポリシー１０に符合すれば、該電子メールがチェック不要メールであることを表すため、該電子メールを送信する。仮に符合しなければ、該電子メールをブロックする。チェック不要メールの設定によって、企業のセキュリティポリシーによるチェック不要扱いの対象を設定することができる。チェック不要扱いの対照には、例えば本社、子会社、重要な顧客、取引のあるメーカー、講読するメールマガジンを提供するドメインネーム、もしくは固定ＩＰ、もしくは企業が許可することによって、企業内部の構成員が企業の外部から受信する電子メール（例えば従業員の家庭、下請け工場、特別な外部の連絡地点など）等が挙げられ、およそ企業がチェック不要扱いとする対象は、優先して送信する。

【００４１】

エージェントの採取する行為は、電子メールポリシーに設定される内容によって、それぞれ相反する結果が表われる。即ち、電子メールポリシーがスパムメール行為をシミュレートしたものであれば、ポリシーに符合した場合、電子メールをブロックし、電子メール

ポリシーがチェック不要のメール行為をシミュレートしたものであれば、ポリシーに符合した場合、メールを通過させる。但し、そのワークの原理は同様である。よって、スパムメールの管理、制御のプロセスについて以下詳細に説明を行い、チェック不要メールのシミュレートについては詳述しない。

【００４２】

スパムメールの管理、制御を例に挙げると、電子メールが電子メールポリシー１０に符合するか否か認証する場合のステップは、図３に開示する通りである。即ち、エージェントが電子メールを受け取ると、第１の電子メールポリシーに基づいて該電子メールのメール伝送データについて真偽を認証し、該第１の電子メールポリシーに符合するか判断する。符合するのであればＳ１２のステップに進み、該電子メールの送信を許可する。符合しなければＳ１４のステップに進む。

【００４３】

Ｓ１４のステップにおいて、エージェントは第２の電子メールポリシーに基づき、電子メールのルートを遡り、継続して認証を行い、第２の電子メールポリシーに符合するか否か判断する。符号するのであればＳ１２のステップに進み、該電子メールの送信を許可する。符合しなければＳ１６のステップに進み、電子メールポリシーに従って該電子メールのルートを継続して遡り、最後の電子メールポリシーに至るまで続ける。

【００４４】

Ｓ１８のステップにおいて、最後の電子メールポリシーに至り、該電子メールを認証した場合、仮に該電子メールが最後の電子メールポリシーに符合すれば、Ｓ１２のステップに進み、仮に該電子メールがやはり電子メールポリシーのルールに符合しなければ、該電子メールが確かに送信を許可することにできないものであることを確認し、Ｓ２０のステップに進む。Ｓ２０のステップにおいて、エージェントは適宜な行為を採取して、該電子メールを送信しないようにする。

【００４５】

電子メールを送信しない場合の処理方法は、電子メールの受信を拒絶し、エラーコードとエラーメッセージを返信するか、もしくは該電子メールを直接削除する。電子メールを送信しない場合の処理方法は、電子メールポリシーを設定する場合、予め指定することができる。

【００４６】

また、図３に開示するプロセスにおいて、メールポリシーに基づいて電子メールの送信データについて認証を行う場合のステップを、図２を参考にして以下に詳述する。

（ａ）第１のルールに従って電子メールの送信データについて、真偽を認証し、第１のルールに符合するか否か判断する。符合するのであれば次の（ｂ）のステップに進み、符合しない場合は（ｃ）のステップへ進む。

（ｂ）第２のルールに従い、継続して該電子メールの送信データの真偽を認証し、第２のルールに符合するか否か判断する。符合するのであれば次の（ｃ）のステップに進み、符合しないのであれば、次のルールに従って該電子メールのルートを遡って認証を行い、最後のルールに至るまで継続して行う。また、最後のルールによる認証結果に基づいて、該電子メールがメールポリシーに符合するか否か決定する。符合するのであれば該電子メールの伝送を許可し送信する。符合しない場合は（ｃ）のステップに進む。

（ｃ）次のメールポリシー内の規則に従い、該電子メールのルートを継続して遡り、メールポリシーに符合するか否か判断する。符合するのであれば、該電子メールの伝送を許可して送信する。符合しないのであれば，次のメールポリシーによって該電子メールのルートを継続して遡り、最後のメールポリシーを適用するまで継続する。

【００４７】

従って、この発明は電子メールの全面的な、且つ重要なデータを掌握して管理を行うものであって、メール行為、及びその処理方法について正確に設定することによって電子メールを効率よく管理する目的を達成することができる。

【００４８】

スパムメールは匿名、偽称、乱発、非合法（データの変動、またはデータの隠匿）などの行為をもって電子メールを送信するものである。この点において、ルートを遡り、送信者を知ることができ、且つ正式なルートを経て講読を取り消す権利を広告用のメールと異なる。送信者が故意に匿名、偽称、乱発、或いは非合法（データの変動、またはデータの隠匿など）などの行為をもって電子メールを送信するのであれば、恐らく乱発されたスパムメールであると認識することができる。

【００４９】

上述するメールポリシーは、電子メールがスパムメールであるか否か判断するために用いられ、その判断は該電子メールが通常と異なる行為によるものか否かの判断を依拠とする。通常と異なる行為とは、匿名、偽称、乱発、または非合法などの行為であって、認証によって該電子メールが通常とことなる行為によるものであるものと認めた場合、これをスパムメールと判断する。例えば匿名にする行為には、ヘッダのデータが不明瞭であるか、送信者のコンピュータと返信の宛先のコンピュータとが異なるか、または返信の宛先のコンピュータがインターネットサーバープロバイダのコンピュータであるといった行為が含まれる。偽称する行為には、送信元のコンピュータが外部のドメインにありながら、送信者のアドレスを該ドメイン内のコンピュータのものであると偽称するか、もしくはドメインのドメインネームサーバが不正確であるなどの行為を指す。乱発する行為とは、送信方法が異常で、且つ頻繁に変動することを指す。非合法方の行為とは、返信するアドレスがレンタルしたコンピュータのものであることを指す。

【００５０】

匿名行為の分析について、この発明の方法は上述する匿名の行為を判断するのみならず、機械的に送信したものか、ハッカーが送信したものか、または人的に送信した電子メールであるか判別することができる。例えばポストマスター（Ｐｏｓｔｍａｓｔｅｒ）の送信した電子メールか、メーラーデイモン（ｍａｉｌｅｒｄｅｍｏｎ）の送信したものか、リストサーバー（Ｌｉｓｔｓｅｒｖｅｒ）が送信した電子メールであるか、等を判断することができる。

【００５１】

この発明によるスパムメール行為の分析を利用した電子メールの管理・制御方法は、通常エージェント内で実施される。比較的よく利用されるのはメールメール集配信サーバー（ＭＴＡ）である。ＭＴＡの実行段階で予め設定したスパムメール行為をシミュレートしてメールエンベロープ、メールヘッダなどの情報を把握し、かつ遡ってメール伝送データの真偽性を分析して当該行為が「スパムメール行為」に該当するかどうかを正確に検証する。また、該ＭＴＡはルータであってもよい。

【００５２】

以下、三種類の具体的な実例を挙げて、この発明の方法による効果を立証し、かつ当業者が本発明を実施するための依拠となるように、詳細に説明する。

【００５３】

第１の実例は、電子メールの送受信の管理・制御を行う場合であって、内部の特定の使用者だけが電子メールを内部の特定の使用者に送信することができるものである。その画面の表示は表１のとおりである。

【表１】

スタート　エンベロープ情報：ルール間の関連性が[AND]で、全て符合して条件が成立する。			
☑ エンベロープ送信者	照合項目 Host	含む／含まない ＋	アドレスリストの選択 特定の内部で使用
☑ エンベロープ受信者	照合項目 Host	含む／含まない －	アドレスリストの選択 特定の内部で使用
	○照合する	◎無視する	
メールヘッダー			
スタート　エンベロープ情報：ルール間の関連性が[AND]で、全て符合して条件が成立する。			
□照合項目 Header 符合条件	要件 Element	比較方法 Method	含む／含まない ＋/－
	◎符合する　○符合しない　以上のポリシーは、次の処理を行う。		
処理方法	◎受信を拒絶してエラーコードとエラーメッセージを返信する。 ○電子メールを削除してエラーコードとエラーメッセージを返信しない。 ○直接伝送する。		

【００５４】

第２の実例は、スパムメールをブロックする場合である。匿名行為の場合は、例えば送信者のホストコンピュータと返信するメールボックスが異なる。その画面の表示は表２のとおりである。

【表２】

スタート　エンベロープ情報：ルール間の関連性が[AND]で、全て符合して条件が成立する。			
□エンベロープ送信者	照合項目	含む／含まない	アドレスリストの選択
□エンベロープ受信者	Envelop From 照合項目 Envelop To	＋/－ 含む／含まない ＋/－	アドレスリストの選択
メールヘッダー	○照合する	◎無視する	
スタート　エンベロープ情報：ルール間の関連性が[AND]で、全て符合して条件が成立する。			
☑ 照合項目 From	要件 Host	照合方法 Cache	含む／含まない ＋/－
			アドレスリストの選択又はユーザー自身で入力
☑ 照合項目 Return-Path	要件 Host	照合方法 Match Cache	含む／含まない ＋/－
			アドレスリストの選択又はユーザー自身で入力
	◎符合する　○符合しない　以上のポリシーは、次の処理を行う。		
符合条件			
処理方法	◎受信を拒絶してエラーコードとエラーメッセージを返信する。 ○電子メールを削除してエラーコードとエラーメッセージを返信しない。 ○直接伝送する。		

【００５５】

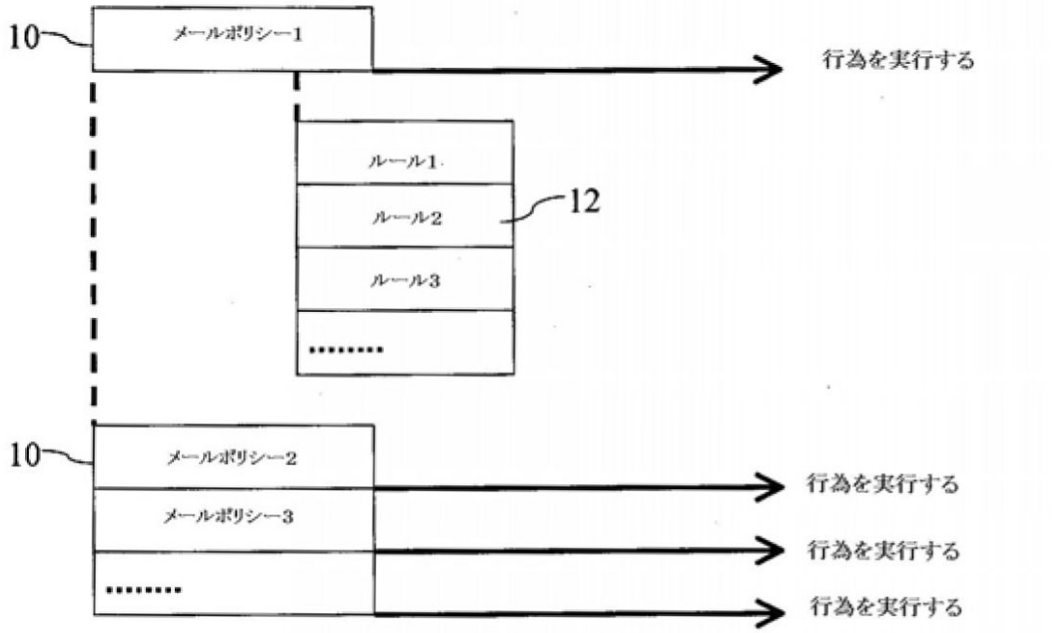
第３の実例は、スパムメールをブロックする場合であって、偽称行為は、例えば発信元のホストコンピュータが外部のインターネットエリアに在りで、送信者のアドレスが内部のホストコンピュータであるように偽称している。その画面の表示は表３のとおりである。

【表３】

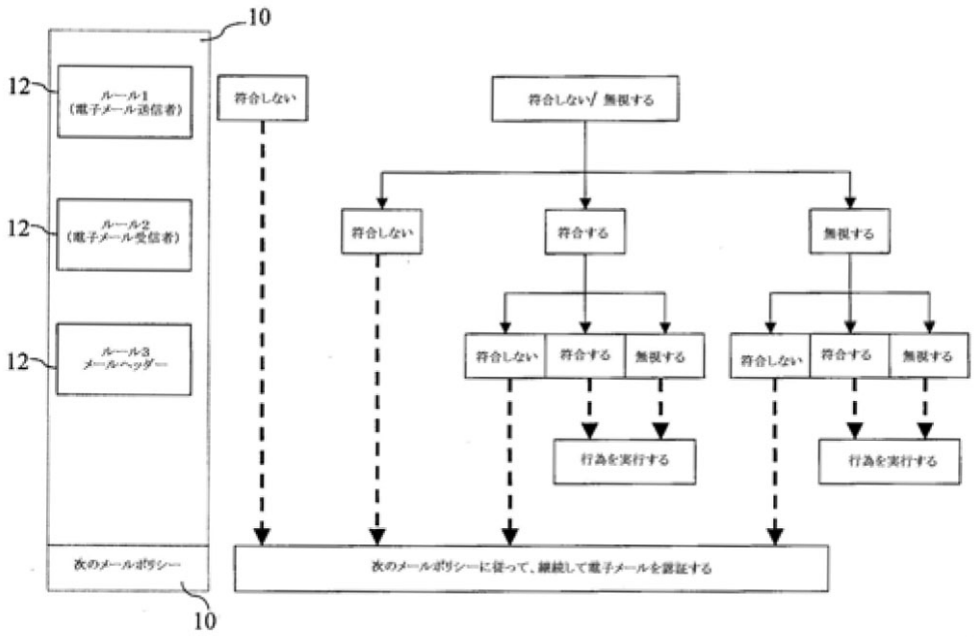
スタート　エンベロープ情報：ルール間の関連性が[AND]で、全て符合して条件が成立する。			
□ エンベロープ送信者	照合項目 Envelop From	含む／含まない +/−	アドレスリストの選択
□ エンベロープ受信者	照合項目 Envelop To	含む／含まない +/−	アドレスリストの選択
メールヘッダー　○照合する　◎無視する			
スタート　エンベロープ情報：ルール間の関連性が[AND]で、全て符合して条件が成立する。			
照合項目	要件	比較方法	含む／含まない　アドレスリストの選択又はユーザー自身で入力
☑ Sender	Sender Domain Host	−	内部ホストコンピュータ
照合項目	要件	比較方法	含む／含まない　アドレスリストの選択又はユーザー自身で入力
☑ From	Sender Domain Host	+	内部ホストコンピュータ
符合条件	◎符合する　○符合しない		以上のポリシーは、次の処理を行う。
処理方法	◎受信を拒絶してエラーコードとエラーメッセージを返信する。 ○電子メールを削除してエラーコードとエラーメッセージを返信しない。 ○直接伝送する。		

【００５６】
この発明は電子メールの特性及び送信の原則を利用して電子メールの「エンベロープ」、「ヘッダ」などメールの伝送データの真偽性を分析し、且つ反復して認証し、認証する電子メールが予め設定したメールポリシーの許可するものであるか、正確に帰納と演繹を行って電子メールの管理と制御を行うとともに、スパムメールをブロックする作用を達成する。よって、この発明は、電子メールの管理と制御を正確に行うとともに、スパムメールを確実にブロックすることができ、ネットワークの安全性を高めるのみならず、ネットワークの帯域と、システムのリソースと、ハードディスクの空間を節約することができ、電子メールの通信効率を高め、運営コストを低減させることができる。
【００５７】
以上は、この発明の好ましい実施例であって、この発明の実施の範囲を限定するものではない。よって、当業者のなし得る修正、もしくは変更であって、この発明の精神の下においてなされ、かつこの発明に対して均等の効果を有するものは、いずれもこの発明の特許請求の範囲に含まれるものとする。
【図面の簡単な説明】
【００５８】
【図１】この発明による電子メールの管理、制御方法を示した説明図である。
【図２】この発明におけるメールポリシーの設定を示した説明図である。
【図３】この発明においてメールポリシーに従って電子メールを認証するステップを示したフローチャトである。
【符号の説明】
【００５９】
１０　メールポリシー
１２　ルール

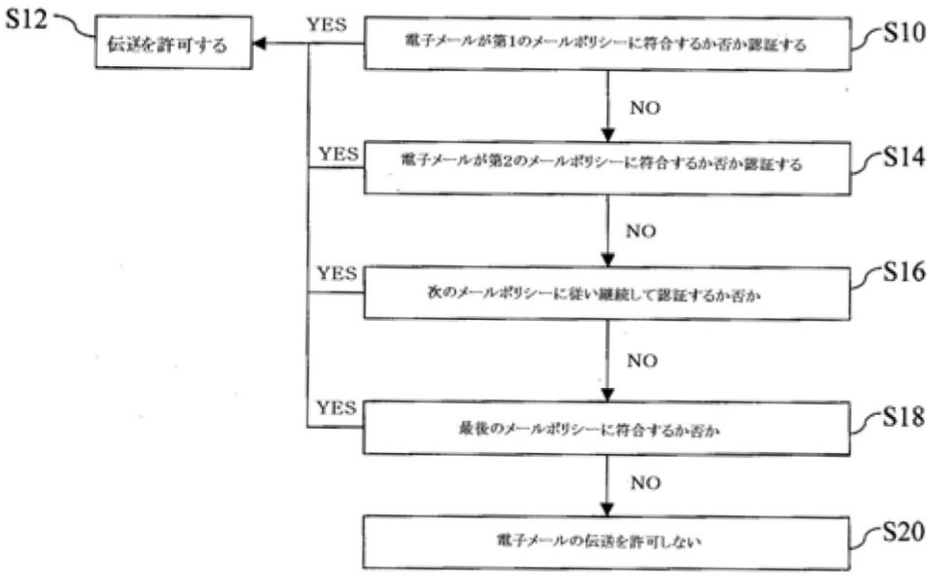
【図１】


10
メールポリシー1
行為を実行する
ルール1
ルール2
12
ルール3
10
メールポリシー2
行為を実行する
メールポリシー3
行為を実行する
行為を実行する

【図２】


10
12
ルール1
(電子メール送信者)
12
ルール2
(電子メール受信者)
12
ルール3
メールヘッダー
符合しない
符合しない/ 無視する
符合しない
符合する
無視する
符合しない
符合する
無視する
符合しない
符合する
無視する
行為を実行する
行為を実行する
次のメールポリシー
次のメールポリシーに従って、継続して電子メールを認証する
10

【図３】


S12
伝送を許可する
YES
電子メールが第1のメールポリシーに符合するか否か認証する
S10
NO
YES
電子メールが第2のメールポリシーに符合するか否か認証する
S14
NO
YES
次のメールポリシーに従い継続して認証するか否か
S16
NO
YES
最後のメールポリシーに符合するか否か
S18
NO
電子メールの伝送を許可しない
S20