(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4335582号
(P4335582)
(45)発行日　平成21年9月30日(2009.9.30)　(24)登録日　平成21年7月3日(2009.7.3)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 610Q
G06F 21/00 (2006.01)　　G06F 15/00 330Z

請求項の数 24　(全 30 頁)

(21)出願番号　特願2003-148320(P2003-148320)
(22)出願日　平成15年5月26日(2003.5.26)
(65)公開番号　特開2004-30639(P2004-30639A)
(43)公開日　平成16年1月29日(2004.1.29)
審査請求日　平成18年4月17日(2006.4.17)
(31)優先権主張番号　10/180,565
(32)優先日　平成14年6月26日(2002.6.26)
(33)優先権主張国　米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　98052-6399　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(74)復代理人　100115635
弁理士　窪田　郁大
(72)発明者　ジョシュア　セオドア　グッドマン
アメリカ合衆国　98052　ワシントン州　レッドモンド　ノースイースト　38　ストリート　17424
最終頁に続く

(54)【発明の名称】迷惑電子メールを検出するシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
迷惑電子メールを簡単に検出できるようにするシステムであって、
スパム通信に関連する複数の特徴を格納する電子メールコンポーネントであって、電子メールメッセージを受信または格納し、前記関連する複数の特徴の各々が前記受信または格納された電子メールメッセージに含まれるか否かに基づいて前記各特徴を要素とする特徴ベクトルを生成し、該生成された特徴ベクトルを用いて前記電子メールメッセージがスパムである確率を判定する電子メールコンポーネントと、
スパムである確率が第１のしきい値よりも大きい電子メールメッセージの送信側に応答を求めるチャレンジを送信するチャレンジコンポーネントであって、前記チャレンジに対する応答に基づいて前記電子メールメッセージがスパムである確率を変更するチャレンジコンポーネントとを備えることを特徴とするシステム。
【請求項２】
前記チャレンジには前記チャレンジにコードが埋め込まれており、前記送信側に前記埋め込まれたコードで応答を要求するものであることを特徴とする請求項１に記載のシステム。
【請求項３】
前記チャレンジは前記送信側に計算を要求する計算チャレンジを送信する計算チャレンジであることを特徴とする請求項１に記載のシステム。
【請求項４】

前記計算チャレンジはタイムスタンプおよび受信者スタンプを含む前記メッセージの一方向ハッシュであることを特徴とする請求項３に記載のシステム。
【請求項５】
前記チャレンジは前記送信側に人間の操作に基づく応答を要求する人間チャレンジであることを特徴とする請求項１に記載のシステム。
【請求項６】
前記チャレンジは前記送信側に対する決済の要求情報を含むことを特徴とする請求項１に記載のシステム。
【請求項７】
前記チャレンジは前記送信側が正当な応答を返信する難しさが異なる複数のチャレンジを含み、前記チャレンジコンポーネントにより送信されるチャレンジの難しさは、前記電子メールメッセージがスパムである確率に基づくことを特徴とする請求項１に記載のシステム。
【請求項８】
迷惑メッセージを簡単に検出できるようにするシステムであって、
スパムに含まれることが予想される複数の特徴を格納し、着信メッセージを受け取り、前記予想される複数の特徴の各々が前記着信メッセージに含まれるか否かに基づいて前記各特徴を要素とする特徴ベクトルを生成し、該生成された特徴ベクトルを用いて前記着信メッセージがスパムである確率を判定し、前記確率に基づいて前記着信メッセージをスパムまたは正当なメッセージとして分類し、前記着信メッセージをスパムフォルダまたは正当なメッセージフォルダに格納するメールクラシファイヤと、
前記メッセージがスパムと分類された場合に前記メッセージの送信側に応答を求めるチャレンジを送信するチャレンジコンポーネントであって、前記チャレンジに対する応答に基づいて前記着信メッセージを前記スパムフォルダから前記正当なメールフォルダに移動するチャレンジコンポーネントとを備えることを特徴とするシステム。
【請求項９】
前記チャレンジには前記チャレンジにコードが埋め込まれており、前記送信側に前記埋め込まれたコードで応答を要求するものであることを特徴とする請求項８に記載のシステム。
【請求項１０】
前記チャレンジは前記送信側に計算を要求する計算チャレンジであることを特徴とする請求項８に記載のシステム。
【請求項１１】
前記チャレンジは前記送信側に人間の操作に基づく応答を要求する人間チャレンジであることを特徴とする請求項８に記載のシステム。
【請求項１２】
前記チャレンジは前記送信側に対する決済の要求情報を含むことを特徴とする請求項８に記載のシステム。
【請求項１３】
正当なメッセージの送信者に関連する情報を格納する正当なメッセージ送信者記憶領域をさらに備えることを特徴とする請求項８に記載のシステム。
【請求項１４】
前記チャレンジに対して正しい応答があった場合に前記チャレンジコンポーネントは前記メッセージの前記送信者に関連する情報を前記正当なメッセージ送信者記憶領域に追加することを特徴とする請求項１３に記載のシステム。
【請求項１５】
スパムの送信者に関連する情報を格納するスパム送信者記憶領域をさらに備えることを特徴とする請求項８に記載のシステム。
【請求項１６】
迷惑電子メールを簡単に検出できるようにするシステムであって、

スパム電子メールに関連する複数の特徴を格納し、着信電子メールメッセージを受け取り、前記関連する複数の特徴の各々が前記着信電子メールメッセージに含まれるか否かに基づいて前記各特徴を要素とする特徴ベクトルを生成し、該生成された特徴ベクトルを用いて前記着信電子メールメッセージがスパムである確率を生成し、前記確率に基づいて前記着信電子メールメッセージをスパム、疑わしいスパム、または正当な電子メールとして分類し、前記着信メッセージをスパムフォルダ、疑わしいスパムフォルダ、または正当なメールフォルダに格納するメールクラシファイヤと、

疑わしいスパムと分類された電子メールメッセージの送信側に応答を求めるチャレンジを送信するチャレンジコンポーネントであって、前記チャレンジに対する応答に基づいて前記着信電子メールメッセージを前記疑わしいスパムフォルダから前記スパムフォルダまたは前記正当なメールフォルダに移動するチャレンジコンポーネントとを備えることを特徴とするシステム。

【請求項１７】

前記チャレンジは応答を要求するために埋め込まれた埋め込みコード、前記送信側に計算を要求する計算チャレンジ、前記送信側に人間の操作に基づく応答を要求する人間チャレンジ、および前記送信側に対する決済の要求情報を含む決済要求のうち少なくとも１つであることを特徴とする請求項１６に記載のシステム。

【請求項１８】

正当な電子メールの送信者に関連する情報を格納する正当な電子メール送信者記憶領域をさらに備えることを特徴とする請求項１６に記載のシステム。

【請求項１９】

スパムの送信者に関連する情報を格納するスパム送信者記憶領域をさらに備えることを特徴とする請求項１６に記載のシステム。

【請求項２０】

前記電子メールメッセージは受信者別ＩＤを含むことを特徴とする請求項１６に記載のシステム。

【請求項２１】

前記チャレンジコンポーネントはさらに、前記電子メールメッセージがメーリングリストからのものかどうかを検出するように適合されることを特徴とする請求項１６に記載のシステム。

【請求項２２】

前記チャレンジコンポーネントはさらに、前記メーリングリストが監査役付きかまたは監査役付きでないかを検出するように適合されることを特徴とする請求項２１に記載のシステム。

【請求項２３】

請求項１に記載の電子メールチャレンジに応答する方法であって、

電子メールメッセージへの応答を求めるチャレンジを受信するステップと、

処理されるチャレンジの量が少ないメッセージを、処理されるチャレンジの量が多いメッセージよりも先に処理されるように、前記チャレンジを順序付けるステップと、

前記チャレンジの量が少ないメッセージの前記チャレンジを処理するステップと、

前記チャレンジの量が少ないメッセージの前記チャレンジへの応答を送信するステップとを備えることを特徴とする方法。

【請求項２４】

迷惑電子メールを簡単に検出できるようにするシステムであって、

予め定義されたスパムに関連する複数の特徴の各々が受信または格納された電子メールメッセージに含まれるか否かに基づいて前記各特徴を要素とする特徴ベクトルを生成し、該生成された特徴ベクトルを用いて電子メールメッセージがスパムである確率を取得する手段と、

前記確率が第１のしきい値よりも大きい電子メールメッセージの送信者に応答を求めるチャレンジを送信する手段と、

前記チャレンジに対する応答に基づいて、前記電子メールメッセージがスパムである確率を変更する手段とを備えることを特徴とするシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、一般に、電子メール（ｅメール）に関するものであり、より具体的には、チャレンジ（Ｃｈａｌｌｅｎｇｅ）を使用した迷惑メール（ｓｐａｍ）検出を採用するシステムおよび方法に関する。

【０００２】

【従来の技術】

電子メッセージ通信、特にインターネットで伝送される電子メール（「ｅメール」）は、急速に社会に普及してきているだけでなく、その非公式性、使い勝手、安価であることから、多くの個人および組織にとって好ましい通信形態となりつつある。

【０００３】

しかし残念なことに、従来の通信形態（例えば、郵便や電話）でもあったように、電子メール受信者に大量の迷惑メール（ｕｎｓｏｌｉｃｉｔｅｄ　ｍａｉｌｉｎｇ）が届く機会が次第に増えてきている。インターネットベースの商取引が特にここ数年の間に爆発的に増えるとともに、さまざまな電子商取引業者（ｅｌｅｃｔｒｏｎｉｃ　ｍｅｒｃｈａｎｄｉｓｅｒ）が自社製品およびサービスを宣伝する迷惑メールを、たえず増え続ける多くの電子メール受信者に繰り返し送りつけている。インターネットを介して製品を注文したり、あるいは他の方法で業者と取り引きするほとんどの消費者は、このような業者からの勧誘を受け取ることを期待しており、また実際に恒常的に受け取っている。しかし、電子メールソフト（ｅｌｅｃｔｒｏｎｉｃ　ｍａｉｌｅｒ）は絶えずその配布リストを拡大することで社会により深く浸透し、受信者の数をますます増やしている。例えば、受信者はさまざまなＷｅｂサイトによって生成される訪問者情報（ｖｉｓｉｔｏｒ　ｉｎｆｏｒｍａｔｉｏｎ）のおそらく差し障りのないようにみえる要求に応えて電子メールアドレスを入力したにすぎないのに、多くの場合、後で迷惑メールを受け取ってから、きわめて不愉快なことに、電子メール配布リストに加えられたことを知るのである。このような状況は、同意している人はともかくとして、受信者についての知識がなくても生じる。さらに、郵便のダイレクトメールリストと同様、電子メールソフトは、多くの場合販売、リース、またはその他の手段により、配布リストを他の同様の電子メールソフトに広め、次々に他の電子メールソフトに広めてゆく。そうこうしているうちに電子メール受信者は、ますます多様化するさまざまな多数のメールソフトが保持する別個の配布リストで生成される迷惑メールの集中砲火を浴びることになりがちである。ダイレクトメール業界には、業界全体の相互協力のもとで、個人が自分の名前をダイレクトメールの郵便リスト（ｐｏｓｔａｌ　ｌｉｓｔｓ）から削除する要求を出すための手段がいくつか存在してはいるが、電子メールソフトにはこのようなメカニズムは存在していない。

【０００４】

受信者が自分が電子メールのメーリングリストに載っていることに気づいても、個人では、自分のアドレスを削除しようにも容易でなく、実際にはそれ以降も迷惑メールが続き、多くの場合、そのリストからますます大量のメールが届き、さらには他のリストからも届くことになる。これは、送信者側でメッセージの受信者がそのメッセージの送信者を特定できなくし（プロキシサーバを通してメールを送信するなどして）、そうすることで受信者が送信者と接触して配布リストからの削除を試みることができないようにしたり、あるいは受信者からすでに受信している除外要求を単に無視するという単純な理由による。

【０００５】

１年以内に数百通の迷惑郵便を個人が受け取ることは十分あり得る。それとは対照的に、電子配布リスト（ｅ－ｄｉｓｔｒｉｂｕｔｉｏｎ　ｌｉｓｔ）は簡単にやり取りでき、電子メールメッセージを非常に多くのアドレスにまき散らすことにもほとんどコストがかからないことから、複数の配布リストに登録されている単一の電子メールアドレスに、きわ

めて短時間のうちに膨大な数の迷惑メッセージが届くことが予想される。さらに、多数の迷惑電子メールメッセージ（例えば、事務用品やコンピュータ補給品の値引き売り込み、あれやこれやの会議出席勧誘）は悪意のないものであるが、ポルノグラフィ、扇情的で不正なものなどは受信者によっては非常に不快なものとなりうる。

【０００６】

迷惑電子メールメッセージは一般に「スパム」と呼ばれる。迷惑郵便物を取り扱う作業の場合と同じようにして、電子メール受信者は着信メールを選り分けてスパムを取り除かなければならない。残念なことに、与えられた電子メールメッセージがスパムかそうでないかの選り分け方は、特定の受信者とメッセージの内容により大きく異なり、ある受信者にとってはスパムであっても別の受信者にとってはスパムでない場合がある。電子メールソフトは、その真の内容が件名行だけでは明らかでなく、メッセージの本文を読まないとわからないようなメッセージを作成することが多い。したがって、受信者は、スパムメッセージを完全に除去するためには、件名行をただ読み飛ばしていくのではなく、受け取った各メッセージをすべて最後まで読むという厄介な作業を行うことになる。言うまでもないが、このようなフィルタ処理（手作業で行うことが多い）は根気がいる、時間のかかる作業である。

【０００７】

不正なニュースグループメッセージ（いわゆる「フレーム（ｆｌａｍｅｓ）」）を検出する作業を自動化するため、ルールベースのテキストクラシファイヤ（ｔｅｘｔ　ｃｌａｓｓｉｆｉｅｒ）を通じてニュースグループメッセージを分類するアプローチを教示する技術がある（例えば、非特許文献１参照）。ここで、意味論および文法に基づくテキスト分類の特徴を、まず、確率的意志決定ツリージェネレータ（ｐｒｏｂａｂｉｌｉｓｔｉｃ　ｄｅｃｉｓｉｏｎ　ｔｒｅｅ　ｇｅｎｅｒａｔｏｒ）を通じて、ニュースグループメッセージの適切なコーパスをトレーニングセット（ｔｒａｉｎｉｎｇ　ｓｅｔ）として供給することにより決定する。これらのメッセージをそれぞれ「フレーム」であるかないかを手作業で分類すると、ジェネレータが、メッセージ内に存在していようといまいと、一般にメッセージがフレームであるかないかを予測することができるテキストの具体的特徴について線引きを行う。次に、後で使用するため十分に高い確率でメッセージの性質を正しく予測できる特徴を選択する。それ以降、着信メッセージを分類するために、そのメッセージ内の各センテンスを処理して、各要素は単にそのセンテンス内の異なる特徴の有無を示すだけの複数要素（例えば、４７要素）特徴ベクトル（ｆｅａｔｕｒｅ　ｖｅｃｔｏｒ）を出力する。メッセージ内のすべてのセンテンスの特徴ベクトルを総和して、（メッセージ全体の）メッセージ特徴ベクトルを出力する。次に、メッセージ特徴ベクトルを意思決定ツリージェネレータにより生成された対応するルールを通じて評価し、メッセージ全体に存在するかまたは存在しない特徴の組合せおよび数に応じて、メッセージがフレームであるかそうでないかを判別する。例えば、作成者は、一意味論的特徴として、単語「ｙｏｕ」が「ｙｏｕ　ｐｅｏｐｌｅ」、「ｙｏｕ　ｂｏｚｏｓ」、「ｙｏｕ　ｆｌａｍｅｒｓ」などの語句で修飾されている語句は侮辱的な意味を持つ傾向があること気づく。例外は、「ｙｏｕ　ｇｕｙｓ」という語句で、使用されていても滅多に侮辱的意味を持たない。したがって、このような前者の語句が存在するかどうかが１つの特徴となる。関連するルールは、このような語句が存在する場合、センテンスは侮辱的なものであり、メッセージはフレームであるというものである。他の特徴は、「ｎｏ　ｔｈａｎｋｓ」ではなく「ｔｈａｎｋ」、「ｐｌｅａｓｅ」、または単語「ｗｏｕｌｄ」を含む（「Ｗｏｕｌｄ　ｙｏｕ　ｂｅ　ｗｉｌｌｉｎｇ　ｔｏ　ｅ−ｍａｉｌ　ｍｅ　ｙｏｕｒ　ｌｏｇｏ」など）語句構文が存在することである。このような語句または単語が存在する場合（「ｎｏ　ｔｈａｎｋｓ」を除く）、作成者が「礼儀正しさルール（ｐｏｌｉｔｅｎｅｓｓ　ｒｕｌｅ）」として参照する関連するルールではそのメッセージを礼儀正しいものとして分類し、したがってフレームではないものとして分類する。いくつかの例外はあるが、このアプローチで使用するルールは、サイト固有ではなく、つまり、大部分、メール送信先のアドレスに関係なく同じ特徴を使用し、同じ方法で作用する。

【０００８】
ルールベースの電子メールクラシファイヤ、ここで特に学習した「キーワード発見ルール（ｋｅｙｗｏｒｄ－ｓｐｏｔｔｉｎｇ　ｒｕｌｅｓ）」に関連するものについては、非特許文献２（これ以降、「Ｃｏｈｅｎ」刊行物と呼ぶ）で説明されている。このアプローチでは、すでにさまざまなカテゴリに分類されている一組の電子メールメッセージがシステムに入力として与えられる。すると、この一組の電子メールメッセージからルールを学習して着信電子メールメッセージをさまざまなカテゴリに分類する。この方法にはルールの自動生成を行うための学習コンポーネントが必要であるが、これらのルールでは、与えられた予測に対する信頼度測定基準（ｃｏｎｆｉｄｅｎｃｅ　ｍｅａｓｕｒｅ）を設定せずに電子メールメッセージをさまざまなカテゴリに分類するためにｙｅｓ／ｎｏの区別を単に行うだけである。さらに、この作業では、スパム検出を行うことの実際の問題には触れていない。この点に関して、ルールベースのクラシファイヤには、実際にスパム検出での使用をひどく制限することになるいろいろな重大な欠陥がある。まず、既存のスパム検出システムでは、ユーザが手作業で、まともなメールとスパムメールとを区別する適切なルールを構築する必要がある。ほとんどの受信者は、このような骨の折れる作業をわざわざしない。上記のように、特定の電子メールメッセージがスパムであるかそうでないかを評価することは、受信者の主観にかなり依存する。一方の受信者にとってはスパムであっても、別の受信者にはスパムでないこともある。さらに、スパムでないメールは人によりかなり違う。したがって、ルールベースクラシファイヤが着信メールストリームからほとんどのスパムを削除する条件を満たす性能を持つためには、受信者側でスパムを構成するものとスパムでない（正当な）電子メールを構成するものとを正確に区別する一組の分類ルールを構築しプログラムしなければならない。適切な動作を行わせることは、経験と知識が豊富なコンピュータユーザであってもきわめて複雑で、単調で、時間のかかる作業になる可能性がある。

【０００９】
第２に、スパム電子メールとスパムでない電子メールの特徴は時間とともに大きく変化する可能性があり、ルールベースクラシファイヤは（ユーザがすすんでいつもルールに変更を加えていない限り）静的なものである。したがって、大量電子メール送信者は自分が送るメッセージの内容を定期的に変更し、受信者がこれらのメッセージをスパムとしてはじめに認識してしまい、全部読み終えないうちにメッセージを破棄するのを防止する（「裏をかく」）努力を絶えず続けている。そのため、受信者自らが絶えず新しいルールを構築するかまたは既存のルールを更新してスパムの変更を追跡する（その受信者がそのような変更を認識したときに）ことをしないと、時間がたつうちに、ルールベースクラシファイヤは、その受信者宛てに来たスパムと望んでいる（スパムでない）電子メールとを正確に区別することが次第にできなくなり、それによりさらにクラシファイヤの効用が減じ、ユーザ／受信者が苛立たしい思いをすることになる。

【００１０】
それとは別に、ユーザ側で既存のスパムから（Ｃｏｈｅｎ刊行物に示されているような）ルールを学習し、時間の経過とともに着信電子メールストリームの変更に対応する方法を考えることもできる。ここで、ルールベースのアプローチの問題はさらにはっきりと際立つ。ルールは論理式に基づいており、したがって、上述のように、ルールは単に与えられた電子メールメッセージの分類に関するｙｅｓ／ｎｏの区別を出力するだけである。問題なのは、このようなルールから、予測に関してどのようなレベルの信頼性も得られないという点である。電子メールからのスパム除去に対する要望の強さに関してユーザにはさまざまな許容範囲があるため、スパムを検出などのアプリケーションにおいて、ルールベースの分類にはかなり問題があるであろう。例えば、慎重なユーザであればメッセージがスパムである確度が非常に高いことが破棄する前にわかるシステムを必要とするが、別のユーザの場合はそれほど注意深くない。ユーザの予防措置はこのように程度に差があるため、Ｃｏｈｅｎ刊行物に記述されているようなルールベースシステムに組み込むことは簡単にはできない。

【００１１】
【非特許文献１】
E. Spertus "Smokey: Automatic Recognition of Hostile Messages", Proceedings of the Conference on Innovative Applications in Artificial Intelligence (IAAI), 1997
【００１２】
【非特許文献２】
W. W. Cohen, "Learning Rules that Classify E-mail", 1996 AAA1 Spring Symposium on Machine Learning in Information Access, 1996
【００１３】
【発明が解決しようとする課題】
以下では、本発明のいくつかの態様の基本的な内容を理解できるように、本発明の概要を簡単に述べる。この概要は、本発明の概要を広範囲にわたって述べたものではない。この概要は、本発明の鍵となる要素や決定的な要素を示したり、本発明の範囲を定めることを目的としていない。後で提示する詳細な説明の前置きとして本発明のいくつかの概念を簡単に示すことのみを目的とする。
【００１４】
本発明は、迷惑メッセージ（例えば電子メール）の検出を行うシステムを実現する。このシステムは、電子メールコンポーネントおよびチャレンジコンポーネント（ｃｈａｌｌｅｎｇｅ　ｃｏｍｐｏｎｅｎｔ）を含む。システムは、メッセージとメッセージがスパムである関連する確率とを受け取ることができる。システムは、少なくとも一部は関連付けられた確率に基づき、チャレンジをメッセージの送信者に送信することができる。電子メールコンポーネントは、メッセージとメッセージがスパムである関連付けられた確率を格納することができる。一実施例では、電子メールメッセージは、電子メールメッセージがスパムである関連する確率に基づいてフォルダ名などの異なる属性とともに格納される。他の実施例では、関連する確率が第１のしきい値以下である電子メールメッセージを正当な電子メールフォルダに格納し、関連する確率が第１のしきい値よりも大きい電子メールメッセージをスパムフォルダに格納する。本発明のさらに他の実施形態では、関連する確率が第１のしきい値以下である電子メールメッセージを正当な電子メールフォルダに格納し、関連する確率が第１のしきい値よりも大きいが第２のしきい値以下である電子メールメッセージを疑わしいスパムフォルダに格納する。関連する確率が第２のしきい値よりも大きい電子メールメッセージをスパムフォルダに格納する。第１のしきい値および／または第２のしきい値は、ユーザ設定に基づいて固定することができ、かつ／または条件に合わせて変更することもできる（例えば、少なくとも一部は利用可能な計算資源に基づいて）ことは理解されるであろう。
【００１５】
【課題を解決するための手段】
サポートベクトルマシン（Ｓｕｐｐｏｒｔ　Ｖｅｃｔｏｒ　Ｍａｃｈｉｎｅ）やニューラルネットワークの得点など、確率以外の数値を確率と同じ目的に使用することができ、一般に、本発明の一態様により機械学習アルゴリズムの数値出力を確率の代わりに使用できることは理解されるであろう。同様に、意思決定ツリーなどのいくつかの機械学習アルゴリズムはカテゴリ情報を出力し、この情報をしきい値と組み合わせた確率の代わりに使用することもできる。
【００１６】
チャレンジコンポーネントはチャレンジを、関連する確率が第１のしきい値よりも大きい電子メールメッセージの送信者に送信することができる。例えば、チャレンジは、少なくとも一部はチャレンジ内に埋め込まれたコード（例えば、英数字コード）に基づくものにすることができる。このチャレンジに応答して、電子メールの送信者はそのコードで返信することができる。一実施例では、埋め込まれているコードを自動的に取り出し、そのチャレンジに応答するよう送信者のシステムを適合させることができる。それとは別に、かつ／またはそれに対する追加として、送信者がチャレンジに応答するよう送信者に要求

することもできる（例えば、手動で）。埋め込まれたコードに基づいてチャレンジを使用すると、スパムの送信者の帯域幅および／または計算負荷を増やすことができ、したがってこれはスパム送信に対する抑制手段として使用できる。チャレンジにはさまざまな種類のものがあるがそのうち適当なものでよいことは理解されるであろう（例えば、計算チャレンジ（ｃｏｍｐｕｔａｔｉｏｎａｌ　ｃｈａｌｌｅｎｇｅ）、人間チャレンジ（ｈｕｍａｎ　ｃｈａｌｌｅｎｇｅ）、および／または少額決済要求（ｍｉｃｒｏｐａｙｍｅｎｔ　ｒｅｑｕｅｓｔ））。チャレンジは固定でも可変でもよい。例えば、大きくされた関連する確率について、チャレンジコンポーネントがより難しいチャレンジまたはより多額の少額決済を要求するチャレンジを送信することができる。

【００１７】

チャレンジコンポーネントは、少なくとも一部はチャレンジへの応答に基づき電子メールメッセージがスパムである関連する確率を変更することができる。例えば、チャレンジに対する適切な（正しい）応答を受信した後、チャレンジコンポーネントでは、電子メールメッセージがスパムである関連する確率を下げることができる。一実施例では、電子メールメッセージをスパムフォルダから正当な電子メールフォルダに移動する。他の実施形態では、電子メールメッセージを疑わしいスパムフォルダから正当な電子メールフォルダに移動する。チャレンジに対する不適切な（例えば、不正な）応答を受信した後かつ／または一定期間（例えば、４時間）内にチャレンジに対する応答を受け取ることができなかったときに、チャレンジコンポーネントでは電子メールメッセージがスパムである関連する確率を高くすることができる。例えば、電子メールメッセージを疑わしいスパムフォルダからスパムフォルダに移動することができる。

【００１８】

本発明の他の態様では、システムはさらにメールクラシファイヤを含む。メールクラシファイヤは、電子メールメッセージを受け取ると、電子メールメッセージがスパムである関連する確率を求め、電子メールメッセージおよび関連する確率を電子メールコンポーネントに格納する。そこで、メールクラシファイヤはメッセージの内容を指定受信者について分析し、その内容に基づき、その受信者について、スパムと正当な（スパムでない）メッセージとを区別し、その結果、その受信者に対するそれぞれの着信電子メールメッセージを分類する。

【００１９】

それに加えてかつ／またはそれとは別に、電子メールメッセージに、メッセージがスパムである確からしさ（確率）の指標を付けて、その確からしさに基づきスパムの中間確率を割り当てたメッセージを疑わしいスパムフォルダに移動することができる。少なくとも一部は、メールクラシファイヤから得られる情報に基づき、チャレンジコンポーネントはチャレンジを、関連する確率が第１のしきい値よりも大きい電子メールメッセージの送信者に送信することができる。

【００２０】

本発明の他の態様では、システムはさらにスパムフォルダと正当な電子メールフォルダを備える。メールクラシファイヤは、電子メールメッセージがスパムである関連する確率を求め、電子メールメッセージをスパムフォルダまたは正当な電子メールフォルダに（例えば、第１のしきい値に基づいて）格納する。着信電子メールメッセージがメールクラシファイヤの入力に送られ、そこで各メッセージが確率的に正当またはスパムとして分類される。その分類結果に基づき、メッセージをスパムフォルダまたは正当な電子メールフォルダに送る。それ以降、チャレンジコンポーネントはチャレンジを、スパムフォルダに格納されている（例えば、関連する確率が第１のしきい値よりも大きい）電子メールメッセージの送信者に送信することができる。チャレンジコンポーネントは、少なくとも一部はチャレンジへの応答に基づき、電子メールメッセージをスパムフォルダから正当な電子メールフォルダに移動することができる。例えば、チャレンジコンポーネントは、チャレンジへの適切な（例えば正しい）応答を受信した後、電子メールメッセージをスパムフォルダから正当な電子メールフォルダに移動することができる。さらに、チャレンジに対する不

適切な（例えば、不正な）応答を受信した後かつ／または一定期間（例えば、４時間）内にチャレンジに対する応答を受け取ることができなかったときに、チャレンジコンポーネントは、スパムフォルダから電子メールメッセージを削除し、かつ／またはスパムフォルダに格納されている電子メールメッセージの属性を変更することができる。

【００２１】

本発明の他の態様では、システムはさらに正当な電子メール送信者記憶領域（ｌｅｇｉｔｉｍａｔｅ　ｅ－ｍａｉｌ　ｓｅｎｄｅｒ（ｓ）ｓｔｏｒｅ）および／またはスパム送信者記憶領域（ｓｐａｍ　ｓｅｎｄｅｒ（ｓ）ｓｔｏｒｅ）を備える。正当な電子メール送信者記憶領域には、正当な電子メールの送信者と関連する情報（例えば、電子メールアドレス）を格納する。正当な電子メール送信者格記憶域内で識別された送信者からの電子メールメッセージは一般的に、チャレンジコンポーネントによるチャレンジを受けない。情報（例えば、電子メールアドレス）は、ユーザの選択（例えば、「チャレンジを実行しない」という特定の送信者コマンド）、ユーザのアドレス帳、ユーザが少なくとも指定された数の電子メールメッセージを送信した宛先のアドレスに基づき、かつ／またはチャレンジコンポーネントにより正当な電子メール送信者記憶領域に格納することができる。正当な電子メール送信者記憶領域には、さらに、正当な電子メールの送信者に関連する信頼度レベルを格納することができる。関連する確率が送信者の関連する信頼度レベル以下である電子メールメッセージはチャレンジコンポーネントによるチャレンジを受けないが、関連する確率が関連する信頼度レベルよりも大きい電子メールメッセージはチャレンジコンポーネントによるチャレンジを受ける。スパム送信者記憶領域には、スパムの送信者と関連する情報（例えば、電子メールアドレス）を格納する。情報は、ユーザおよび／またはチャレンジコンポーネントがスパム送信者記憶領域に格納することができる。

【００２２】

【発明の実施の形態】

前記の目的および関連する目的を達成するために、以下の説明および添付の図面に関して、本発明のいくつかの態様を図で説明する。ただし、これらの態様は本発明の原理を採用するさまざまな方法のうちわずかのみを示しており、本発明はこのような態様およびその等価物すべてを含むことを意図している。本発明の他の利点および新規性のある特徴は、図面とともに本発明の以下の詳細な説明を読むと明らかになるであろ。

【００２３】

全体を通して同様の参照番号は同様の要素を参照している図面を参照しながら本発明について説明する。以下の説明では、説明のため本発明を完全に理解できるように多数の特定の詳細を定めている。ただし、こうした具体的内容がなくても本発明を実践できることは明白であろう。他の例では、よく知られている構造およびデバイスはブロック図の形式で示されており、本発明を説明しやすくしている。

【００２４】

本出願で使用されているように、「コンピュータコンポーネント」という用語は、コンピュータ関連のエンティティ、ハードウェア、ハードウェアとソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかを指すものとする。例えば、コンピュータコンポーネントとして、限定はしないが、プロセッサ上で実行されているプロセス、プロセッサ、オブジェクト、実行可能ファイル、実行のスレッド、プログラム、および／またはコンピュータを挙げることができる。説明のために、サーバ上で実行されているアプリケーションとそのサーバを両方ともコンピュータコンポーネントとすることができる。１つまたは複数のコンピュータコンポーネントを１つのプロセッサおよび／または実行のスレッド内に常駐させることができ、またコンポーネントを１台のコンピュータにローカルとして配置し、かつ／または２台またはそれ以上のコンピュータ間に分散させることができる。

【００２５】

図１を参照すると、本発明の一態様による迷惑メッセージ（例えば、電子メール）を検出するシステム１００が説明されている。このシステム１００は、電子メールコンポーネン

ト１１０およびチャレンジコンポーネント１２０を備える。システム１００は、電子メールメッセージと電子メールメッセージがスパムである関連する確率を受け取ることができる。システム１００は、少なくとも一部は関連付けられた確率に基づき、チャレンジを電子メールメッセージの送信者に送信することができる。

【００２６】

電子メールコンポーネント１１０は、電子メールメッセージを受信しかつ／または受信メッセージを受け取りかつ／または格納し、かつ／または電子メールメッセージがスパムである関連付する確率を計算する。例えば、電子メールコンポーネント１１０は少なくとも一部は、メールクラシファイヤ（図に示されていない）から受け取った情報に基づき情報を格納することができる。一実施例では、電子メールメッセージは、電子メールメッセージがスパムである関連する確率に基づいて電子メールコンポーネント１１０に格納される。他の実施例では、電子メールコンポーネント１１０は、電子メールメッセージを受信し電子メールメッセージがスパムである関連付する確率を計算する。

【００２７】

チャレンジコンポーネント１２０はチャレンジを、関連する確率が第１のしきい値よりも大きい電子メールメッセージの送信者に送信することができる。例えば、チャレンジは、少なくとも一部はチャレンジ内に埋め込まれたコード（例えば、英数字コード）に基づくものにすることができる。このチャレンジに応答して、電子メールの送信者はそのコードで返信することができる。一実施例では、埋め込まれているコードを自動的に取り出し、そのチャレンジに応答するよう送信者のシステム（図に示されていない）を適合させることができる。それとは別に、かつ／またはそれに対する追加として、送信者がチャレンジに応答するよう送信者に要求することもできる（例えば、手動で）。埋め込まれたコードに基づいてチャレンジを使用すると、スパムの送信者の帯域幅および／または計算負荷を増やすことができ、したがってこれはスパム送信に対する抑制手段として使用できる。

【００２８】

それに加えてかつ／またはそれとは別に、チャレンジを計算チャレンジ、人間チャレンジ、および／または少額決済要求とすることができる。これらのチャレンジおよびチャレンジに対する応答について以下の段落で詳述する。さらに、チャレンジは固定および／または可変とすることができる。例えば、大きくされた関連する確率について、チャレンジコンポーネント１２０がより難しいチャレンジまたはより多額の少額決済を要求するチャレンジを送信することができる。

【００２９】

例えば、オプションにより少額決済要求で１回限りのスパム証明書（ｏｎｅ－ｔｉｍｅ－ｕｓｅ　ｓｐａｍ　ｃｅｒｔｉｆｉｃａｔｅｓ）を使用することもできる。システム１００は、受信したスパム証明書を「保留」にすることができる。システム１００のユーザがメッセージを読み、それにスパムのマークを付けると、スパム証明書が無効化され、送信者はスパム証明書をそれ以上使用することができなくなる。メッセージにスパムのマークが付いていない場合、保留が解除され、送信者はスパム証明書を再利用できるようになる（例えば、メッセージの送信者に課金されない）。他の実施形態では、スパム証明書は、メッセージにスパムのマークがついていようといまいと常に受信時に無効化される。

【００３０】

一実施形態では計算チャレンジに関して、チャレンジ送信者（メッセージ受信者）側で計算チャレンジをどのようなものにすべきかを決定することができる。しかし、他の実施形態では、チャレンジはメッセージの内容、メッセージの受信または送信時刻、メッセージ送信者、および、重要なものとして、メッセージ受信者の何らかの組合せにより一意に決定される。例えば、計算チャレンジは、これらの数量の一方向ハッシュに基づくことができる。チャレンジ送信者（メッセージ受信者）がチャレンジを選択できる場合には、スパマー（ｓｐａｍｍｅｒ）は以下の手法を使用することができるであろう。スパマーは、メーリングリストに加入するか、または他の何らかの手段でユーザからメールを生成する。そこで、応答者はメッセージを、スパマーが自分の選択した計算チャレンジで応答する先

のスパマーに送り返す。特に、スパマーは正当なユーザがすでにスパムに応答してスパマーに送信してしまっているチャレンジを選択することができる。スパマーのチャレンジの受信者の数パーセントがチャレンジを解き、その結果スパマーがスパマーに送信されたチャレンジに解答することができる。一実施形態では、計算チャレンジはメッセージ（時刻および受信スタンプを含む）の一方向ハッシュに基づいており、送信者または受信者がチャレンジを決定することは実質的に不可能であるが、それぞれチャレンジが意図した目的に使用されていることを確認することは可能である。

【００３１】

チャレンジコンポーネント１２０は、少なくとも一部はチャレンジへの応答に基づき電子メールメッセージがスパムである関連する確率を変更することができる。例えば、チャレンジに対する適切な（正しい）応答を受信した後、チャレンジコンポーネント１２０では、電子メールメッセージがスパムである関連する確率を下げることができる。一実施例では、電子メールメッセージをスパムフォルダから正当な電子メールフォルダに移動する。他の実施例では、電子メールメッセージを疑わしいスパムフォルダから正当な電子メールフォルダに移動する。さらに、チャレンジに対する不適切な（例えば、不正な）応答を受信した後かつ／または一定期間（例えば、４時間）内にチャレンジに対する応答を受け取ることができなかったときに、チャレンジコンポーネント１２０では電子メールメッセージがスパムである関連する確率を高くすることができる。

【００３２】

一実施形態では、ユーザにチャレンジの選択権が与えられる。例えば、チャレンジの選択をフィルタに基づくようにできる。

【００３３】

さらに、電子メールメッセージを格納する代わりに、システム１００はメッセージを「宛先不明として送り返す」ことができ、したがって、送信者はチャレンジへの応答でメッセージを再送する必要がある。

【００３４】

図１はシステム１００のコンポーネントを示すブロック図であるが、チャレンジコンポーネント１２０は、本明細書で定義している用語に従い、１つまたは複数のコンピュータコンポーネントとして実装することができる。そこで、本発明によりシステム１００および／またはチャレンジコンポーネント１２０を実装するために動作可能なコンピュータ実行可能コンポーネントを、限定はしないが、ＡＳＩＣ（特定用途向け集積回路）、ＣＤ（コンパクトディスク）、ＤＶＤ（デジタルビデオディスク）、ＲＯＭ（読み取り専用メモリ）、フロッピー（登録商標）ディスク、ハードディスク、ＥＥＰＲＯＭ（電気的消去可能プログラム可能読み取り専用メモリ）、メモリスティックなどのコンピュータ読み取り可能媒体上に格納することができる。

【００３５】

図２を参照すると、本発明の一態様による迷惑電子メールを検出するシステム２００が説明されている。このシステム２００は、電子メールコンポーネント１１０、チャレンジコンポーネント１２０、およびメールクラシファイヤ１３０を含む。メールクラシファイヤ例１３０は、「A TECHNIQUE WHICH UTILIZES A PROBABILISTIC CLASSIFIER TO DETECT "JUNK" E-MAIL」という表題の米国同時係属特許出願第０９／１０２８３７号明細書に詳しく記述されている。一実施例では、メールクラシファイヤ１３０は、電子メールメッセージを受け取ると、電子メールメッセージがスパムである関連する確率を求め、電子メールメッセージおよび関連する確率を電子メールコンポーネント１１０に格納する。メールクラシファイヤ１３０はメッセージの内容を指定受信者について分析し、その内容に基づき、その受信者について、スパムと正当な（スパムでない）メッセージとを区別し、その結果、その受信者に対するそれぞれの着信電子メールメッセージを分類する。

【００３６】

他の実施例では、各着信電子メールメッセージ（メッセージストリーム内の）を最初に分析してから、一組の定義済み特徴、特にスパムの特性のうちのどれがメッセージに含まれ

ているかを評価する。これらの特徴（例えば、「特徴集合（ｆｅａｔｕｒｅ　ｓｅｔ）」）は単純単語ベースの特徴（ｓｉｍｐｌｅ－ｗｏｒｄ－ｂａｓｅｄ　ｆｅａｔｕｒｅｓ）および手作業特徴（ｈａｎｄｃｒａｆｔｅｄ　ｆｅａｔｕｒｅｓ）の両方を含み、後者は、例えば特別な複数単語語句および電子メールメッセージ内の非単語区別などのさまざまな特徴を含む。一般的に、これらの非単語区別は、まとめると、例えば、メッセージ内に存在する場合にスパムであることを示す傾向のあるフォーマッティング、オーサリング、配信、および／または通信属性に関係し、これらはスパムのドメイン特有の特性である。例えば、フォーマッティング属性には、メッセージのテキスト内の定義済み単語が大文字になっているか、そのテキストに一連の定義済み句読点が含まれているかなどの属性が含まれる。例えば、配信属性は、メッセージに単一受信者のアドレスまたは複数の受信者のアドレスまたはメッセージが送信された時刻（真夜中に送信されたメールはスパムである可能性が高い）が含まれるかどうかを示す。例えば、オーサリング属性は、メッセージの送信元が特定の電子メールアドレスかどうかを示す。例えば、通信属性は、メッセージに添付ファイルが含まれるかどうか（スパムメッセージには滅多に添付が含まれない）、あるいはメッセージが特定のドメインタイプの送信者によって送信されたかどうかを示す（ほとんどのスパムは「．ｃｏｍ」または「．ｎｅｔ」ドメインタイプから発信されているようである）。手作業の特徴はさらに、例えば、不正であったり、ポルノグラフィであったり、侮辱的であることが知られているトークンまたは語句、あるいはスパム内にそれぞれ出現する可能性の高い繰り返される感嘆符または数値などのある種の句読点またはグループも含むことができる。特定の手作業の特徴は、通常、人間の判断だけで判別したり、あるいはスパムメッセージの属性を識別する経験的分析と組み合わせることもできる。

【００３７】

集合内の各特徴に１つの要素を有する特徴ベクトルが着信電子メールメッセージ毎に生成される。その要素は単に、対応する特徴がそのメッセージ内に存在するかどうかを指定する２進値を格納するだけである。ベクトルは、疎形式（ｓｐａｒｓｅ　ｆｏｒｍａｔ）で格納することができる（例えば、ポジティブな特徴のリストのみ）。ベクトルの内容を入力として確率的クラシファイヤ、好ましくは、メッセージに存在するまたは存在しない特徴に基づき、メッセージがスパムかそうでないかに関して確率的測定基準（ｐｒｏｂａｂｉｌｉｓｔｉｃ　ｍｅａｓｕｒｅ）を生成する修正サポートベクトルマシン（ｍｏｄｉｆｉｅｄ　ｓｕｐｐｏｒｔ　ｖｅｃｔｏｒ　ｍａｃｈｉｎｅ）（ＳＶＭ）クラシファイヤに適用する。その後、この測定基準をプリセットされたしきい値と比較する。メッセージに関して、その関連する確率的測定基準がしきい値以上の場合、このメッセージはスパムとして分類される（例えば、スパムフォルダに格納される）。それとは別に、このメッセージの確率的測定基準がしきい値未満の場合、メッセージは正当なものとして分類される（例えば、正当なメールフォルダに格納される）。各メッセージの分類は、そのメッセージのベクトル内の別々のフィールドとして格納することもできる。正当なメールフォルダの内容は、ユーザの選択および検討対象となるクライアント電子メールプログラム（図に示されていない）により表示することができる。スパムフォルダの内容は、特定のユーザ要求の後にクライアント電子メールプログラムによってのみ表示される。

【００３８】

さらに、メールクラシファイヤ１３０は、正当なメールまたはスパムのいずれかとしてそれぞれ手動で分類されているＭ個の電子メールメッセージの集合（例えば、Ｍをある整数とした「学習集合」）を使用して学習することができる。特に、これらのメッセージをそれぞれ分析して、単純単語ベースの特徴および手作業による特徴の両方を含むｎ個の可能な特徴からなる比較的大きな普遍集合（ｕｎｉｖｅｒｓｅ）（ここでは「特徴空間（ｆｅａｔｕｒｅ　ｓｐａｃｅ）」と呼ぶ）から後で分類を行うときに使用する特徴集合を含む特定のＮ個の特徴（ただし、ｎおよびＮはｎ＞Ｎを満たす整数である）だけを判別する。特に、後で必要な範囲で詳しく説明するようにＺｉｐｆの法則（Ｚｉｐｆｓ　Ｌａｗ）と相互情報とを適用することで学習集合に対するｎ個すべての特徴の結果を含む行列（通常は疎行列）の大きさを小さくし、縮退（ｒｅｄｕｃｅｄ）Ｎ×ｍ特徴行列を得る。得られ

たＮ個の特徴は、後の分類で使用される特徴集合を形成する。この行列および学習集合内の各メッセージの既知の分類をまとめて、学習のためメールクラシファイヤ１３０に適用する。

【００３９】

さらに、受信者が手動でメッセージを一方のフォルダから他方のフォルダに移動して、分類しなおす場合、例えば、正当な電子メールフォルダからスパムフォルダに移動する場合、いずれかのフォルダまたは両方のフォルダの内容を新しい学習集合としてフィードバックして再学習し、クラシファイヤを更新することができる。このような再学習は、メッセージを再分類する毎に結果として、一定数のメッセージを再分類した後自動的に、所定の使用間隔（例えば、数週間または数カ月）が経過した後、またはユーザからの要求があった後に実行することができる。このようにして、クラシファイヤの動作は特定のユーザの変化する主観的認知および選好を追跡できて都合がよい。それとは別に、電子メールメッセージをスパムの複数のカテゴリ（サブクラス）（例えば、商業スパム、ポルノグラフィスパムなど）に分類することができる。さらに、メッセージをスパムのさまざまな程度（例えば、「特定のスパム」、「疑わしいスパム」、「スパムでない」）に対応するカテゴリに分類することができる。

【００４０】

少なくとも一部は、メールクラシファイヤ１３０から得られる情報に基づき、チャレンジコンポーネント１２０はチャレンジを、関連する確率が第１のしきい値よりも大きい電子メールメッセージの送信者に送信することができる。例えば、チャレンジは、少なくとも一部はチャレンジ内に埋め込まれたコード（例えば、英数字コード）に基づくものにすることができる。このチャレンジに応答して、電子メールの送信者はそのコードで返信することができる。埋め込まれているコードを自動的に取り出し、そのチャレンジに応答するよう送信者のシステム（図に示されていない）を対応させることができる。それとは別に、かつ／またはそれに対する追加として、送信者がチャレンジに応答するよう送信者に要求することもできる（例えば、手動で）。埋め込まれたコードに基づいてチャレンジを使用すると、スパムの送信者の帯域幅および／または計算負荷を増やすことができ、したがってこれはスパム送信に対する抑制手段として使用できる。本発明を実施するのに適したチャレンジであればどのような種類でも（例えば、計算チャレンジ、人間チャレンジ、少額決済要求）使用することができ、このような種類のチャレンジはすべて請求項の範囲内に収まるものであることは理解されるであろう。

【００４１】

チャレンジコンポーネント１２０は、少なくとも一部はチャレンジへの応答に基づき電子メールメッセージがスパムである関連する確率を変更することができる。例えば、チャレンジに対する適切な（例えば、正しい）応答を受信した後、チャレンジコンポーネント１２０では、電子メールメッセージがスパムである関連する確率を下げることができる。

【００４２】

チャレンジに対する不適切な（例えば、不正な）応答を受信した後かつ／または一定期間（例えば、４時間）内にチャレンジに対する応答を受け取ることができなかったときに、チャレンジコンポーネント１２０では電子メールメッセージがスパムである関連する確率を高くすることができる。メールクラシファイヤ１３０を、本明細書でその用語を定義したようなコンピュータコンポーネントとすることができることは理解されるであろう。

【００４３】

図３を参照すると、本発明の一態様による迷惑電子メールを検出するシステム３００が説明されている。このシステム３００は、メールクラシファイヤ３１０、チャレンジコンポーネント３２０、スパムフォルダ３３０、および正当な電子メールフォルダ３４０を含む。一実施形態では、スパムフォルダ３３０および／または正当な電子メールフォルダ３４０は仮想的なものとすることができる、つまり電子メールメッセージ自体を別の場所に格納し電子メールメッセージと関連する情報（例えば、電子メールメッセージへのリンク）を格納することができる。または、他の実施形態では、フォルダではなく、メッセージの

属性を単に設定することができる。

【００４４】

上述のように、メールクラシファイヤ３１０は、電子メールメッセージがスパムである関連する確率を求め、電子メールメッセージをスパムフォルダ３３０または正当な電子メールフォルダ３４０に（例えば、第１のしきい値に基づいて）格納する。着信電子メールメッセージがメールクラシファイヤ３１０の入力に送られ、そこで各メッセージが確率的に正当またはスパムとして分類される。その分類結果に基づき、電子メールメッセージをスパムフォルダ３３０または正当な電子メールフォルダ３４０のいずれかに送る。そこで、関連する確率が第１のしきい値以下である電子メールメッセージを正当な電子メールフォルダ３４０に格納し、関連する確率が第１のしきい値よりも大きい電子メールメッセージをスパムフォルダ３３０に格納する。第１のしきい値は、ユーザ設定に基づいて固定することができ、かつ／または条件に合わせて変更することもできる（例えば、少なくとも一部は利用可能な計算資源に基づいて）。

【００４５】

それ以降、チャレンジコンポーネント３２０はチャレンジを、スパムフォルダに格納されている（例えば、関連する確率が第１のしきい値よりも大きい）電子メールメッセージの送信者に送信することができる。例えば、チャレンジは、少なくとも一部はチャレンジ内に埋め込まれたコード、計算チャレンジ、人間チャレンジ、および／または少額決済要求に基づくものにすることができる。チャレンジコンポーネント３２０は、少なくとも一部はチャレンジへの応答に基づき、電子メールメッセージをスパムフォルダ３３０から正当な電子メールフォルダ３４０に移動することができる。例えば、チャレンジコンポーネント３２０は、チャレンジへの適切な（例えば正しい）応答を受信した後、電子メールメッセージをスパムフォルダ３３０から正当な電子メールフォルダ３４０に移動することができる。

【００４６】

チャレンジに対する不適切な（例えば、不正な）応答を受信した後かつ／または一定期間（例えば、４時間）内にチャレンジに対する応答を受け取ることができなかったときに、チャレンジコンポーネント３２０は、スパムフォルダ３３０から電子メールメッセージを削除し、かつ／またはスパムフォルダ３３０に格納されている電子メールメッセージの属性を変更することができる。例えば、電子メールメッセージの表示属性（例えば、色）を変更し、電子メールメッセージがスパムである確からしさが高くなったことをユーザに知らせることができる。

【００４７】

次に、図４を参照すると、本発明の一態様による迷惑電子メールを検出するシステム４００が説明されている。このシステム４００は、メールクラシファイヤ３１０、チャレンジコンポーネント３２０、スパムフォルダ３３０、および正当な電子メールフォルダ３４０を含む。システム４００はさらに正当な電子メール送信者記憶領域３５０および／またはスパム送信者記憶領域３６０を含む。正当な電子メール送信者記憶領域３５０には、正当な電子メールの送信者と関連する情報（例えば、電子メールアドレス）を格納する。正当な電子メール送信者格記憶域内３５０で識別された送信者からの電子メールメッセージは一般的に、チャレンジコンポーネント３２０によるチャレンジを受けない。そこで、一実施例では、電子メールメッセージの送信者が正当な電子メール送信者記憶領域３５０に格納されていればメールクラシファイヤ３１０によりスパムフォルダ３３０に格納されている電子メールメッセージは正当なメールフォルダ３４０に移動される。

【００４８】

情報（例えば、電子メールアドレス）は、ユーザの選択（例えば、「チャレンジを実行しない」という特定の送信者コマンド）、ユーザのアドレス帳、ユーザが少なくとも指定された数の電子メールメッセージを送信した宛先のアドレスに基づき、かつ／またはチャレンジコンポーネント３２０により正当な電子メール送信者記憶領域３５０に格納することができる。例えば、電子メールメッセージの送信者がチャレンジに正しく応答した後、チ

ャレンジコンポーネント３２０はその送信者に関連する情報（例えば、電子メールアドレス）を正当な電子メール送信者記憶領域３５０に格納することができる。

【００４９】

正当な電子メール送信者記憶領域３５０では、さらに、正当な電子メールの送信者に関連する信頼度レベルを保持することができる。関連する確率が送信者の関連する信頼度レベル以下である電子メールメッセージはチャレンジコンポーネント３２０によるチャレンジを受けないが、関連する確率が関連する信頼度レベルよりも大きい電子メールメッセージはチャレンジコンポーネント３２０によるチャレンジを受ける。例えば、信頼度レベルは、少なくとも一部は送信者の応答したチャレンジの関連する最高確率に基づくものとすることができる。

【００５０】

一実施形態では、少なくとも一部はユーザのアクション（例えば、スパムとして削除された送信者からの電子メールメッセージ）に基づいて送信者を正当な電子メール送信者記憶領域３５０から削除することができる。他の態様によれば、ユーザが１つの電子メールメッセージを送信者に送信した後送信者を正当な電子メール送信者記憶領域３５０に追加するが、これはメーリングリストの場合に有用である。

【００５１】

スパム送信者記憶領域３６０には、スパムの送信者と関連する情報（例えば、電子メールアドレス）を格納する。情報は、ユーザおよび／またはチャレンジコンポーネント３２０によってスパム送信者記憶領域３６０に格納することができる。例えば、ユーザが特定の電子メールメッセージをスパムとして削除した後、電子メールメッセージの送信者に関連する情報をスパム送信者記憶領域３６０に格納することができる。他の実施例では、チャレンジへの応答は正しくなかった、および／またはチャレンジに応答できなかった電子メールメッセージの送信者に関連する情報をスパム送信者記憶領域３６０に格納することができる。

【００５２】

図５では、本発明の一態様による迷惑電子メールを検出するシステム５００が説明されている。システム５００は、メールクラシファイヤ５１０、チャレンジコンポーネント５２０、スパムフォルダ５３０、疑わしいスパムフォルダ５４０、および正当な電子メールフォルダ５５０を含む。上述のように、メールクラシファイヤ５１０は、電子メールメッセージがスパムである関連する確率を求め、電子メールメッセージをスパムフォルダ５３０、疑わしいスパムフォルダ５４０、または正当な電子メールフォルダ５５０に格納する。着信電子メールメッセージがメールクラシファイヤ５１０の入力に送られ、そこで各メッセージが確率的に正当なメールメッセージ、疑わしいスパム、またはスパムとして分類される。その分類結果に基づき、各メッセージをスパムフォルダ５３０、疑わしいスパムフォルダ５４０、または正当な電子メールフォルダ５５０のいずれかに送る。

【００５３】

関連する確率が第１のしきい値以下の電子メールメッセージは正当な電子メールフォルダ５５０内にある。関連する確率が第１のしきい値超、第２のしきい値以下である電子メールメッセージは疑わしいスパムフォルダ５４０内に格納される。さらに、関連する確率が第２のしきい値よりも大きい電子メールメッセージはスパムフォルダ５３０に格納される。第１のしきい値および／または第２のしきい値は、ユーザ基本設定に基づいて固定することができ、かつ／または（例えば、少なくとも一部は利用可能な計算資源に基づいて）適合できることは理解されるであろう。これ以降、チャレンジコンポーネント５２０はチャレンジを、疑わしいスパムフォルダ５４０内に格納されている電子メールメッセージの送信者に送信することができる。例えば、チャレンジは、少なくとも一部はチャレンジ内に埋め込まれたコード、計算チャレンジ、人間チャレンジ、および／または少額決済要求に基づくものにすることができる。

【００５４】

チャレンジコンポーネント５２０は、少なくとも一部はチャレンジへの応答またはそのよ

うな応答がないことに基づき、電子メールメッセージを疑わしいスパムフォルダ５４０から正当な電子メールフォルダ５５０またはスパムフォルダ５３０に移動することができる。例えば、チャレンジコンポーネント５２０は、チャレンジへの適切な（例えば正しい）応答を受信した後、電子メールメッセージを疑わしいスパムフォルダ５４０から正当な電子メールフォルダ５５０に移動することができる。

【００５５】

さらに、チャレンジに対する不適切な（例えば、不正な）応答を受信した後かつ／または一定期間（例えば、４時間）内にチャレンジに対する応答を受け取ることができなかったときに、チャレンジコンポーネント５２０では電子メールメッセージを疑わしいスパムフォルダ５４０からスパムフォルダ５３０に移動することができる。

【００５６】

次に図６を参照すると、本発明の一態様による迷惑電子メールを検出するシステム６００が説明されている。システム６００は、メールクラシファイヤ５１０、チャレンジコンポーネント５２０、スパムフォルダ５３０、疑わしいスパムフォルダ５４０、および正当な電子メールフォルダ５５０を備える。システム６００はさらに正当な電子メール送信者記憶領域５６０および／またはスパム送信者記憶領域５７０を備える。

【００５７】

正当な電子メール送信者記憶領域５６０には、正当な電子メールの送信者と関連する情報（例えば、電子メールアドレス）を格納する。正当な電子メール送信者格記憶域内５６０で識別されたエンティティからの電子メールメッセージは一般的に、チャレンジコンポーネント５２０によるチャレンジを受けない。そこで、一実施例では、電子メールメッセージの送信者が正当な電子メール送信者記憶領域５６０に格納されていればメールクラシファイヤ５１０によりスパムフォルダ５３０または疑わしいスパムフォルダ５４０に格納されている電子メールメッセージは正当なメールフォルダ５５０に移動される。

【００５８】

情報（例えば、電子メールアドレス）は、ユーザの選択（例えば、「チャレンジを実行しない」という特定の送信者コマンド）、ユーザのアドレス帳、ユーザが少なくとも指定された数の電子メールメッセージを送信した宛先のアドレスに基づき、かつ／またはチャレンジコンポーネント５２０により正当な電子メール送信者記憶領域５６０に格納することができる。例えば、電子メールメッセージの送信者がチャレンジに正しく応答した後、チャレンジコンポーネント５２０はその送信者に関連する情報（例えば、電子メールアドレス）を正当な電子メール送信者記憶領域５６０に格納することができる。

【００５９】

正当な電子メール送信者記憶領域５６０には、さらに、正当な電子メールの送信者に関連する信頼度レベルを格納することができる。例えば、関連する確率が送信者の関連する信頼度レベル以下である電子メールメッセージはチャレンジコンポーネント５２０によるチャレンジを受けないが、関連する確率が関連する信頼度レベルよりも大きい電子メールメッセージはチャレンジコンポーネント５２０によるチャレンジを受ける。例えば、信頼度レベルは、少なくとも一部は送信者の応答したチャレンジの関連する最高確率に基づくものとすることができる。

【００６０】

一実施例では、少なくとも一部はユーザのアクション（例えば、スパムとして削除された送信者からの電子メールメッセージ）に基づいて送信者を正当な電子メール送信者記憶領域５６０から削除することができる。他の実施例によれば、ユーザが１つの電子メールメッセージを送信者に送信した後送信者を正当な電子メール送信者記憶領域５６０に追加する。

【００６１】

スパム送信者記憶領域５７０には、スパムの送信者と関連する情報（例えば、電子メールアドレス）を格納する。情報は、ユーザおよび／またはチャレンジコンポーネント５２０によってスパム送信者記憶領域５７０に格納することができる。例えば、ユーザが特定の

電子メールメッセージをスパムとして削除した後、電子メールメッセージの送信者に関連する情報をスパム送信者記憶領域５７０に格納することができる。他の実施例では、チャレンジへの応答は正しくなかった、および／またはチャレンジに応答できなかった電子メールメッセージの送信者に関連する情報をスパム送信者記憶領域５７０に格納することができる。

【００６２】

一実施例では、チャレンジプロセスにおいて一意的ＩＤをやり取りすることができる（例えば、スパマーが善良な送信者のアドレスを使ってスパムを送信する可能性を小さくするため）。さらに、送信者はメッセージ署名を使用することができる。いつもメッセージに署名を入れている正当な電子メール送信者格記憶域内５６０に格納されている送信者から無署名でメッセージが送信された場合、通常の処理および潜在的チャレンジの対象となる。

【００６３】

他の実施例では、大量電子メール送信者は自分の「ｆｒｏｍ」アドレス（例えば、受信者の一意的な「ｆｒｏｍ」アドレス）をカスタマイズする。例えば、「ｆｒｏｍ」アドレスは、送信者に知られているグローバルな秘密鍵に基づき、受信者の電子メールアドレスでハッシュすることができる。それとは別に、受信者用に乱数を生成して格納することもできる。

【００６４】

さらに第３の実施例では、「受信者別ＩＤ」（ｐｅｒ　ｒｅｃｅｐｉｅｎｔ：ＰＲＩＤ）を電子メールメッセージに含める。ＰＲＩＤでは、送信者一意情報を特別なメッセージヘッダフィールドに付加する。ＰＲＩＤは送信者毎に設定する必要はないことは理解されるであろう。したがって、組織内でメールを回覧するときに、正当な電子メール送信者記憶領域５６０への取り込みを継承することができる。ＰＲＩＤは、公開鍵署名システム（例えば、ＯｐｅｎＰＧＰまたはＳ／ＭＩＭＥ）で使用する公開鍵とすることができる。

【００６５】

さらに、（例えば、チャレンジの受信のスケジュール設定を容易にするため）電子メールメッセージの送信者はチャレンジに対する要求を含めることもできる。例えば、電子メールメッセージに「ＣＨＡＬＬＥＮＧＥ＿ＭＥ＿ＮＯＷ：ＴＲＵＥ」ヘッダを入れることができる。これにより、システム６００は自動的にチャレンジを送信し、正しい応答が返ってきたときに送信者を正当な電子メール送信者記憶領域５６０に格納することができる。

【００６６】

メーリングリスト（例えば、監査役付きメーリングリスト（ｍｏｄｅｒａｔｅｄ　ｍａｉｌｉｎｇ　ｌｉｓｔ）および／または監査役付きでないメーリングリスト（ｕｎｍｏｄｅｒａｔｅｄ　ｍａｉｌｉｎｇ　ｌｉｓｔ））から受信した電子メールメッセージを検出するようにチャレンジコンポーネント５２０を適合させることができる。例えば、「Ｐｒｅｃｅｄｅｎｃｅ：ｌｉｓｔ」または「Ｐｒｅｃｅｄｅｎｃｅ：ｂｕｌｋ」などのヘッダ行を、メーリングリストから受信した電子メールメッセージに含めることができる。他の実施例では、チャレンジコンポーネント５２０は、少なくとも一部は、「ｆｒｏｍ」行と異なる「ｓｅｎｄｅｒ」行の検出に基づいて電子メールメッセージがスパムであることを検出する。電子メールメッセージヘッダは通常、２つの異なるｆｒｏｍ行、つまり最上行にある「ｆｒｏｍ」行（例えば、ＳＭＴＰによって使用されるｆｒｏｍコマンドによって挿入されるもの）と「ｆｒｏｍ：」ヘッダフィールド（例えば、ユーザ向けに通常表示されるもの）を含む。これらは複数のメーリングリストについて異なることがある。

【００６７】

一実施例では、チャレンジコンポーネント５２０はメーリングリストからの電子メールメッセージを検出し、正当な電子メール送信者記憶領域５６０内にメーリングリストを入れる機会をユーザに与えることができる。チャレンジコンポーネント５２０はさらに、メーリングリストに関連する信頼度レベルを含めることができる。

【００６８】

メーリングリストに関して取り組むべき課題は、メーリングリストから受信したスパムに似たメッセージによりそのメーリングリストに対してチャレンジのメール嵐（ｍａｉｌ　ｓｔｏｒｍ）が発生する可能性を小さくすることである。このような課題は、リストの種類が異なれば異なる。８つの状況があるが、その多くは同じ解決策で対応できる。特に、メーリングリストは監査役付きの場合と監査役付きでないふつうの場合とがあり、さらにチャレンジに応答する能力のレベルはさまざまである。このため８種類になる。

【００６９】

多くの監査役付きメーリングリストは「ａｐｐｒｏｖｅｄ－ｂｙ」ヘッダを含む。例えば、監査役付きメーリングリストでは、すべてのメッセージが良いメッセージであるか、すべてがスパムであると想定することができる。監査役付きでないリストでは、一部のスパムがメーリングリストに送られる可能性があると想定できる。したがって、監査役付きでないメーリングリストでは、チャレンジコンポーネント５２０により、ユーザ側で、スパムに似たメッセージを表示するか、または単純にスパムフォルダ５３０に格納するかを決定するしきい値を設定することができる。

【００７０】

例えば、メーリングリストからの電子メールが検出され、ユーザはメーリングリストに関連する信頼度レベルを決定する機会が与えられる。問題は、メーリングリスト、特にチャレンジに自動的に応答する能力を持たないメーリングリストに多くのチャレンジを送りすぎるという点である。例えば、監査役付のメーリングリストでは、ユーザはメーリングリストを正当な電子メール送信者記憶領域５６０に入れるよう要求される場合がある。他の実施例では、メーリングリストは、チャレンジコンポーネント５２０からのチャレンジに応答することができ、またこのメーリングリストは、正当な電子メール送信者記憶領域５６０に入れることができる。第３の実施例では、メーリングリストを購読するようになった後、メーリングリストをユーザの正当な電子メール送信者記憶領域５６０に入れるようメーリングリストからユーザに対して要求がある。

【００７１】

監査役付でないメーリングリストでは、例えば、ユーザはメーリングリストのしきい値を設定するよう求められる。スパムである確率がしきい値を超える電子メールメッセージは、スパムフォルダ５３０に移動され、かつ／または削除される。他の実施例では、メーリングリストは、チャレンジコンポーネント５２０からのチャレンジに応答することができ、またこのメーリングリストは、正当な電子メール送信者記憶領域５６０に入れることができる。第３の実施例では、メーリングリストを購読するようになった後、メーリングリストをユーザの正当な電子メール送信者記憶領域５６０に入れるようメーリングリストからユーザに対して要求がある。

【００７２】

チャレンジコンポーネント５２０は、チャレンジに自動的に応答する能力を持たないメーリングリストを考慮することができる。特に、監査役付のメーリングリストでは、チャレンジコンポーネント５２０は、メーリングリストを正当な電子メール送信者記憶領域５６０に入れることができる。監査役付きでないメーリングリストでは、チャレンジコンポーネント５２０によりメーリングリストのしきい値が設定しやすくなり、このしきい値を超えるメッセージに対してチャレンジが行われ、このしきい値を下回るメッセージは通す。

【００７３】

正当な電子メール送信者記憶領域５６０への格納は適切な時期に行われる。メーリングリストでは、ユーザがリストにメールを送信しない可能性がある。しかし、リストから受信した少量のメールに基づいてメーリングリストを正当な電子メール送信者記憶領域５６０に格納することは望ましくない。そうしないと、スパマーはメーリングリストの振りをし、少量のメッセージ（いずれもスパムとして削除されていない）を送信し、スパムを自由に送信することができる。一実施形態では、最初にメーリングリストからそのメールが届いたときに、ユーザは、関連するしきい値とともにメーリングリストを正当な電子メール送信者記憶領域５６０に追加するよう要求される。ほとんどのメーリングリストは歓迎メ

ッセージを用意しているため、学習データに歓迎メッセージがいくつか含まれている場合、その歓迎メッセージがスパムとしてマークされる可能性はない。

【００７４】

しかし、到着した最初のメッセージが実質的にすべて、スパムに似ている場合、メッセージをスパムフォルダ５３０に格納すべきである。特に、誰かにメーリングリストの振りをさせ、スパムを送信させることは望ましいことではない。したがって、メーリングリストは正当な電子メール送信者記憶領域５６０に格納されるまで、チャレンジコンポーネント５２０は上述のようにチャレンジをメーリングリストに送信することができる。メッセージがスパムに似てはいるが正当なものである場合、ユーザはチャレンジの処理の仕方に応じて受け入れるかまたは受け入れない場合がある。チャレンジに答えないと通らない。したがって、スパムを通すことは困難であろう。最後に、メーリングリストはスパムでないように見えるメッセージを送信し、ユーザに、メーリングリストの方針を確立するよう要求する。

【００７５】

メーリングリストにＦｒｏｍアドレスがあり、それによりＦｒｏｍアドレスに送信されたメールがリスト全体に送信されることは理解されるであろう。リストがそのようなタイプに見える場合、メーリングリストの実質的にすべての読者が受信するであろうときにチャレンジを送信するのは望ましくない。メーリングリストを正当な電子メール送信者記憶領域５６０に入れる前にこのようなメーリングリストから明らかにわかるスパムは単に無視されるだけである。正当な電子メール送信者記憶領域５６０に入れることの定義は、メーリングリストについて修正することができる。メーリングリスト上のＦｒｏｍ行が与えられた場合、監査役付きのメーリングリストであっても送信者毎に異なり、正当な電子メール送信者記憶領域５６０への格納はヘッダの他の部分に基づくことができる。多くの場合、メーリングリストのＴｏ行はメーリングリスト名である（したがって、ｒｅｐｌｙ－ａｌｌがリスト全体に入る）。そこで、メーリングリストでは、正当な電子メール送信者記憶領域５６０に格納する場合は、少なくとも一部はｔｏ－ｌｉｎｅに基づく。これは、ｆｒｏｍ－ｌｉｎｅリスティングに加えることもできる（例えば、メーリングリストの送信者が十分でもなければならない正当な電子メール送信者記憶領域５６０に格納されている場合）。メーリングリストでは、ｓｅｎｔ－ｂｙなどの他のヘッダ行を正当な電子メール送信者記憶領域５６０にさらにかつ／またはそれとは別に格納できることは理解されるであろう。

【００７６】

電子メールアドレスが有効なものかどうかを判別するために、スパマーは「宛先不明で戻ること」を信頼する。多くの従来の電子メールサーバは、宛先が無効なアドレスの場合に電子メールをその送信者に戻す。そのため、電子メールサーバでは、電子メールメッセージが宛先不明で戻って来るということがない場合に電子メールアドレスが有効かどうかを示す値を大きくする。したがって、スパマーは宛先不明で戻ってくるということのないアドレスにより多くのスパムメッセージを送信することができる。

【００７７】

電子メールを宛先不明で戻すこれらの電子メールサーバの場合、本発明のチャレンジは付加情報をスパマーにいっさい提供しない（例えば、宛先不明で戻ることがないということはアドレスが有効であることを示す）。さらに、電子メールサーバは自動的にシステム経由でチャレンジを送信し、「半分生きている」アドレス（例えば、有効だが監視されていないアドレス）の迷惑電子メールを検出することができる。

【００７８】

電子メールを宛先不明で無効なアドレスへ返すことのない電子メールサーバに関してもやはり、電子メールサーバは迷惑電子メールを検出するため自動的にシステム経由でチャレンジを送信し、例えば、無効なアドレスの振る舞いを有効なアドレスの振る舞いに似たものにすることができる。さらに、一実施形態では、サーバシステムによって、電子メールがスパムである確率にランダム化係数が加算される（例えば、適応型スパムフィルタ（ａ

ｄａｐｔｉｖｅ　ｓｐａｍ　ｆｉｌｔｅｒ）を回避する試みを防止するため）。

【００７９】

次に、図７を参照すると、本発明の一態様によるチャレンジに応答するシステム７００が説明されている。システム７００は、チャレンジ受信コンポーネント７１０、チャレンジプロセッサコンポーネント７２０、およびチャレンジ応答コンポーネント７３０を備える。

【００８０】

チャレンジ受信コンポーネント７１０は、チャレンジを受信する（例えば、すでに送信されている電子メールに）。例えば、チャレンジは、少なくとも一部はチャレンジ内に埋め込まれたコード、計算チャレンジ、人間チャレンジ、および／または少額決済要求に基づくものにすることができる。

【００８１】

一実施例では、チャレンジ受信コンポーネント７１０は、複数のチャレンジモダリティ（ｃｈａｌｌｅｎｇｅ　ｍｏｄａｌｉｔｉｅｓ）のうちのどれをチャレンジプロセッサコンポーネント７２０に転送するかを決定する（例えば、使用可能な計算資源および／またはユーザ設定に基づいて）。他の実施例では、チャレンジ受信コンポーネント７１０は、複数のチャレンジモダリティのうちの１つの選択をしやすくする情報をユーザに送り、それにより、ユーザはチャレンジに応答するために使用したいモダリティ（ｍｏｄａｌｉｔｙ）がもしあればそれを選択することができる。例えば、チャレンジ受信コンポーネント７１０は、ユーザが計算チャレンジへの応答に必要な計算資源の量、少額決済の金額、および／または少額決済勘定残高などの適切な応答モダリティを選択するのに役立つと思われる情報を提供することができる。チャレンジモダリティが選択された後、チャレンジがチャレンジプロセッサ７２０に転送される。

【００８２】

状況によっては、ユーザがチャレンジに応答したくない場合もあり、そのときには、チャレンジプロセッサコンポーネント７２０および／またはチャレンジ応答コンポーネント７３０に情報が送信されないことは理解されるであろう。

【００８３】

チャレンジプロセッサコンポーネント７２０は、チャレンジを処理し、処理されたチャレンジに関連する出力を供給する。例えば、チャレンジに埋め込みコードが含まれる場合、チャレンジプロセッサコンポーネント７２０は出力をその埋め込みコードが含まれるチャレンジ応答コンポーネント７３０に供給することができる。チャレンジに計算チャレンジが含まれる場合、チャレンジプロセッサコンポーネント７２０により計算チャレンジへの解を容易に生成することができる。

【００８４】

チャレンジに人間チャレンジが含まれる場合、チャレンジプロセッサコンポーネント７２０は人間チャレンジを解きやすくする情報をユーザに提供することができる。一実施例では、人間チャレンジに、人間の手で比較的解きやすく、コンピュータでは比較的難しい問題を含めることができる。一実施例では、人間チャレンジに単語のイメージ（例えば、ＧＩＦまたはＪＰＥＧ）を入れる。この単語は、一部ノイズにより分かりにくくされている。このノイズのおかげで、単語を読み取るコンピュータプログラムを自動的に開発する（または少なくとも、既製コンポーネントを使用する）ことが困難になるが、人間が読み取ることはさほど困難ではない。この実施例では、チャレンジプロセッサコンポーネント７２０は単語のイメージをユーザに提供することができる。ユーザは単語をチャレンジプロセッサコンポーネント７２０に送り返す。チャレンジプロセッサコンポーネント７２０は、単語を含む出力をチャレンジ応答コンポーネント７３０に渡す。

【００８５】

チャレンジに少額決済要求が含まれる場合、チャレンジプロセッサコンポーネント７２０は出力をチャレンジ応答コンポーネント７３０に供給する操作を円滑にできる。一実施例では、少額決済チャレンジへの応答は、発行機関（ｉｓｓｕｉｎｇ　ａｕｔｈｏｒｉｔｙ

）が発行できる１回限りの「スパム証明書」に基づく。チャレンジプロセッサコンポーネント７２０は、自動的にまたはユーザ入力に基づいて、スパム証明書番号をチャレンジ応答コンポーネント７３０に渡す。スパム証明書番号を与えることにより、それ以降スパム証明書は無効化される（例えば、１回限りの使用）。

【００８６】

他の実施例では、少額決済チャレンジへの応答は少額決済勘定（ｍｉｃｒｏｐａｙｍｅｎｔ　ａｃｃｏｕｎｔ）に基づく。このような応答がそれぞれあると、例えば、発行機関により、保持されている少額決済講座から一定金額が差し引かれる。チャレンジプロセッサコンポーネント７２０は、少額決済勘定に関連する情報をチャレンジ応答コンポーネント７３０に渡すことができる。

【００８７】

チャレンジ応答コンポーネント７３０は、少なくとも一部は、処理されたチャレンジに関連する出力に基づいてチャレンジへの応答を送る。例えば、チャレンジへの応答には、埋め込みコード、計算チャレンジの解、人間チャレンジの解、および／または少額決済を含めることができる。

【００８８】

一実施形態では、例えば、サービス拒否攻撃の可能性を低減するために、所定のメッセージについてすでに処理されているチャレンジの数量で計算チャレンジの順番が決められる。処理されるチャレンジが少ないメッセージは、処理されるチャレンジが多いメッセージの処理の前に処理される（例えば、計算資源が使用できるので）。したがって、メッセージがメーリングリスト宛てに送信された場合、受信者は悪意をもってサービス拒否攻撃を行おうと計算チャレンジを送信することも可能である。しかし、そのメッセージに対して１つまたは複数の計算チャレンジを処理した後、処理されるチャレンジが少ない他のメッセージの計算チャレンジを優先し、サービス拒否の可能性を抑えることができる。

【００８９】

図に示されている上述のシステム例を見ると、本発明により実装できる方法は図８、９、１０、および１１の流れ図を参照すればよく理解されるであろう。説明を簡単にするために、これらの方法を図に示し、一連のブロックとして記述するが、本発明はブロックの順序によって制限されるわけではなく、本発明により、いくつかのブロックはその図に示されているここで説明しているのと異なる順序で、かつ／または他のブロックと同時に配置することも可能である。さらに、本発明によりこの方法を実装するために図に示されているすべてのブロックが必要なわけではない。

【００９０】

本発明は、１つまたは複数のコンポーネントによって実行されるプログラムモジュールなどのコンピュータ実行可能命令の一般的文脈において説明できる。一般に、プログラムモジュールには、特定のタスクを実行する、あるいは特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、データ構造などが含まれる。通常、さまざまな実施形態で説明されているようにプログラムモジュールの機能を組み合わせるか、または分散させることができる。

【００９１】

図８および９を参照すると、本発明の一態様による迷惑電子メールメッセージを検出する方法８００が説明されている。８０４で、電子メールメッセージを受信する。８０８で、電子メールメッセージがスパムである確率を求める（例えば、メールクラシファイヤにより）。

【００９２】

８１２で、電子メールメッセージの送信者が正当な電子メール送信者記憶領域に入っているかどうかに関して判別する。８１２での判別結果がＹＥＳであれば、処理は８１６から続く。８１２での判別結果がＮＯであれば、８２０で電子メールメッセージの送信者がスパム送信者記憶領域に入っているかどうかに関して判別する。８２０での判別結果がＹＥＳであれば、８２４での処理に続く。８２０での判別結果がＮＯであれば、８２８で電子

メールメッセージの送信者がスパムである確率が第１のしきい値よりも大きいかどうかに関して判別する。８２８での判別結果がＮＯであれば、８１６での処理に続く。８２８での判別結果がＹＥＳであれば、８３２で１つまたは複数のチャレンジが電子メールメッセージの送信者宛てに送信される。

【００９３】

８３６で、チャレンジへの応答を受信したかどうかを判別する。８３６での判別結果がＮＯであれば、８３６での処理に続く。８３６での判別結果がＹＥＳであれば、８４０でチャレンジに対して受信した応答が正しいかどうかを判別する。８４０での判別結果がＹＥＳであれば、８１６での処理に続く。８４０での判別結果がＮＯであれば、８２４での処理に続く。

【００９４】

８１６で、電子メールメッセージが「スパムでない」と識別される（例えば、正当な電子メールフォルダに置かれる、かつ／または関連する確率が引き下げられる）。次に、８４４で、電子メールメッセージの送信者が正当な電子メール送信者記憶領域に追加され、それ以上処理は行われない。

【００９５】

８２４で、電子メールメッセージがスパムと識別される（例えば、スパムフォルダに置かれ、削除され、かつ／または関連する確率が高められる）。次に、８４８で、電子メールメッセージの送信者が正当なスパム送信者記憶領域に追加され、それ以上処理は行われない。

【００９６】

次に、図１０を参照すると、本発明の一態様によるチャレンジに応答する方法１０００が説明されている。１０１０で、電子メールメッセージが送信される。１０２０で、チャレンジを受信する（例えば、埋め込みコード、計算チャレンジ、人間チャレンジ、および／または少額決済の要求）。１０３０で、チャレンジが処理される。１０４０で、チャレンジへの応答が送信される。

【００９７】

次に、図１１を参照すると、本発明の一態様によるチャレンジに応答する方法１１００が説明されている。１１１０で、電子メールメッセージが送信される。１１２０で、チャレンジを受信する（例えば、埋め込みコード、計算チャレンジ、人間チャレンジ、および／または少額決済の要求を含む各チャレンジ）。１１３０で、処理すべきチャレンジの順番は、少なくとも一部は、処理されるチャレンジが少ないメッセージを処理されるチャレンジが多いメッセージよりも先にすることに基づいて決められる（例えば、サービス拒否攻撃を低減するため）。１１４０で、チャレンジが処理される。１１５０で、選択されたチャレンジへの応答が送信される。１１６０で、処理するチャレンジがまだあるかどうかについて判別する。１１６０での判別結果がＹＥＳであれば、処理は１１３０から続く。１１６０での判別結果がＮＯであれば、これ以上処理は行われない。

【００９８】

図１２を参照すると、本発明の一態様による複数のチャレンジに応答するユーザインターフェイス例１２００が説明されている。このユーザインターフェイス例では、以下のメッセージにユーザは促される。

【００９９】

THE E-MAIL MESSAGE YOU SENT HAS BEEN
DETECTED AS POTENTIAL SPAM. UNLESS YOU
CORRECTLY RESPOND TO ONE OF THE
CHALLENGES IDENTIFIED BELOW, THE E-MAIL
MESSAGE MAY BE IDENTIFIED AS SPAM AND/OR
DELETED AS SPAM.

ユーザに対して、コンピュータ計算チャレンジ、人間チャレンジ、および少額決済の３つのオプションが用意される。少なくとも一部はユーザの選択に基づき、選択されているチ

ャレンジを処理することができる。

【０１００】

本発明のさまざまな態様の背景を示すために、図１３および以下の説明では、本発明のさまざまな態様を実装する適当な動作環境１３１０の概要を簡潔に説明する。本発明は、１つまたは複数のコンピュータまたは他のデバイスで実行される、プログラムモジュールなどのコンピュータ実行可能命令の一般的な文脈において説明されているが、当業者であれば、本発明は他のプログラムモジュールと組合せかつ／またはハードウェアとソフトウェアとの組合せとして実装できることも理解するであろう。しかし、一般に、プログラムモジュールには、特定のタスクを実行する、あるいは特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などが含まれる。動作環境１３１０は、適当な動作環境の一例にすぎず、本発明の使用または機能の範囲に関する制限を示唆しないことを意図している。本発明とともに使用するのに適していると思われる他のよく知られているコンピュータシステム、環境、および／または構成は、パーソナルコンピュータ、ハンドヘルドまたはラップトップデバイス、マルチプロセッサシステム、マイクロプロセッサベースシステム、プログラム可能家電製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ、上記システムまたはデバイスを含む分散コンピューティング環境などを含む。

【０１０１】

図１３を参照すると、本発明のさまざまな対応を実装するための環境例１３１０はコンピュータ１３１２を備える。コンピュータ１３１２は、処理装置１３１４、システムメモリ１３１６、およびシステムバス１３１８を含む。システムバス１３１８は、システムメモリ１３１６などのシステムコンポーネントを処理装置１３１４に結合する。処理装置１３１４は、さまざまな市販プロセッサがあるがそのうちどれでもよい。デュアルマイクロプロセッサおよびその他のマルチプロセッサアーキテクチャも、処理装置１３１４として採用することができる。

【０１０２】

システムバス１３１８は、メモリバスまたはメモリコントローラ、周辺機器バスまたは外部バス、および／または、１３ビットバス、Ｉｎｄｕｓｔｒｉａｌ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＩＳＡ）、Ｍｉｃｒｏ－Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ（ＭＳＡ）、Ｅｘｔｅｎｄｅｄ ＩＳＡ（ＥＩＳＡ）、Ｉｎｔｅｌｌｉｇｅｎｔ Ｄｒｉｖｅ Ｅｌｅｃｔｒｏｎｉｃｓ（ＩＤＥ）、ＶＥＳＡ Ｌｏｃａｌ Ｂｕｓ（ＶＬＢ）、Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ（ＰＣＩ）、Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ（ＵＳＢ）、Ａｄｖａｎｃｅｄ Ｇｒａｐｈｉｃｓ Ｐｏｒｔ（ＡＧＰ）、Ｐｅｒｓｏｎａｌ Ｃｏｍｐｕｔｅｒ Ｍｅｍｏｒｙ Ｃａｒｄ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ａｓｓｏｃｉａｔｉｏｎ ｂｕｓ（ＰＣＭＣＩＡ）、およびＳｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｆａｃｅ（ＳＣＳＩ）を含むがこれらには限定されない利用可能な各種バスアーキテクチャを使用するローカルバスを含む数種類のバス構造のうちのいずれかでよい。

【０１０３】

システムメモリ１３１６は、揮発性メモリ１３２０および不揮発性メモリ１３２２を含む。起動時などにコンピュータ１３１２内の要素間の情報転送を行うための基本ルーチンを含む基本入出力システム（ＢＩＯＳ）は、不揮発性メモリ１３２２に格納される。例として、ただしこれらに限られないが、不揮発性メモリ１３２２には、読み取り専用メモリ（ＲＯＭ）、プログラム可能ＲＯＭ（ＰＲＯＭ）、電気的プログラム可能ＲＯＭ（ＥＰＲＯＭ）、電気的消去可能ＲＯＭ（ＥＥＰＲＯＭ）、またはフラッシュメモリなどがある。揮発性メモリ１３２０には、外部キャッシュメモリとして動作するランダムアクセスメモリ（ＲＡＭ）がある。例として、ただしこれらに限られないが、使用可能なＲＡＭには、シンクロナスＲＡＭ（ＳＲＡＭ）、ダイナミックＲＡＭ（ＤＲＡＭ）、シンクロナスＤＲＡＭ（ＳＤＲＡＭ）、Ｄｏｕｂｌｅ Ｄａｔａ Ｒａｔｅ ＳＤＲＡＭ（ＤＤＲＳＤＲＡＭ）、Ｅｎｈａｎｃｅｄ ＳＤＲＡＭ（ＥＳＤＲＡＭ）、Ｓｙｎｃｈｌｉｎｋ ＤＲＡＭ（

ＳＬＤＲＡＭ）、およびＤｉｒｅｃｔ　Ｒａｍｂｕｓ　ＲＡＭ（ＤＲＲＡＭ）などさまざまな形態のものがある。

【０１０４】

コンピュータ１３１２はさらに、取り外し可能／取り外し不可能な揮発性／不揮発性コンピュータ記憶媒体も含む。図１３は、例えばディスク記憶装置１３２４を示している。ディスク記憶装置１３２４には、磁気ディスクドライブ、フロッピー（登録商標）ディスクドライブ、テープドライブ、Ｊａｚドライブ、Ｚｉｐドライブ、ＬＳ－１００ドライブ、フラッシュメモリカード、またはメモリスティックなどがあるがこれらには限定されない。さらに、ディスク記憶装置１３２４は、記憶媒体を単独に含むことも、コンパクトディスクＲＯＭデバイス（ＣＤ－ＲＯＭ）、ＣＤ書き込み可能ドライブ（ＣＤ－Ｒドライブ）、ＣＤ書き換え可能ドライブ（ＣＤ－ＲＷドライブ）、またはデジタル多用途ディスクＲＯＭドライブ（ＤＶＤ－ＲＯＭ）などの光ディスクドライブをはじめとする他の記憶媒体と組み合わせて含むこともできるが、これらには限定されない。ディスク記憶装置１３２４をシステムバス１３１８に接続しやすくするために、通常、インターフェイス１３２６などの取り外し可能または取り外し不可能インターフェイスを使用する。

【０１０５】

図１３は、ユーザと適当な動作環境１３１０内の説明されている基本コンピュータ資源との媒介手段として動作するソフトウェアを説明していることは理解されるであろう。このようなソフトウェアとして、オペレーティングシステム１３２８がある。オペレーティングシステム１３２８は、ディスク記憶装置１３２４に格納することができ、コンピュータシステム１３１２の資源の制御・割り当てを行う働きをする。システムアプリケーション１３３０は、システムメモリ１３１６またはディスク記憶装置１３２４に格納されているプログラムモジュール１３３２およびプログラムデータ１３３４を通じてオペレーティングシステム１３２８により資源の管理を利用する。本発明は、さまざまなオペレーティングシステムまたはオペレーティングシステムの組合せで実装できることは理解されるであろう。

【０１０６】

ユーザは入力デバイス１３３６を使用してコマンドまたは情報をコンピュータ１３１２に入力する。入力デバイス１３３６には、マウスなどのポインティングデバイス、トラックボール、ペン、タッチパッド、キーボード、マイク、ジョイスティック、ゲームパッド、衛星放送受信アンテナ、スキャナ、ＴＶチューナーカード、デジタルカメラ、デジタルビデオカメラ、Ｗｅｂカメラなどがある。これらの入力デバイスやその他の入力デバイスは、インターフェイスポート１３３８を介してシステムバス１３１８を通じ処理装置１３１４に接続する。例えば、インターフェイスポート１３３８にはシリアルポート、パラレルポート、ゲームポート、およびユニバーサルシリアルバス（ＵＳＢ）などがある。出力デバイス１３４０では、入力デバイス１３３６と同じ種類のポートをいくつか使用する。したがって、例えば、ＵＳＢポートを使用して、コンピュータ１３１２に入力し、コンピュータ１３１２からの情報を出力デバイス１３４０に出力することができる。出力アダプタ１３４２が備えられており、特別なアダプタを必要とする他の出力デバイス１３４０のうちモニタ、スピーカ、およびプリンタなどいくつかの出力デバイスがあることを示している。出力アダプタ１３４２は、例えば、これらに限られられないが、出力デバイス１３４０とシステムバス１３１８とを接続する手段となるビデオおよびサウンドカードなどがある。他のデバイスおよび／またはデバイスのシステムはリモートコンピュータ１３４４などの入出力機能を備えることに留意されたい。

【０１０７】

コンピュータ１３１２は、リモートコンピュータ１３４４などの１つまたは複数のリモートコンピュータへの論理接続を使用してネットワーク環境で動作させることができる。リモートコンピュータ１３４４は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ワークステーション、マイクロプロセッサベース機器、ピアデバイス、またはその他の共通ネットワークノードなどでよく、通常は、コンピュータ１３１２に関係する上

述の要素の多くまたはすべてを含む。簡単のため、メモリ記憶装置１３４６のみリモートコンピュータ１３４４とともに示してある。リモートコンピュータ１３４４は、ネットワークインターフェイス１３４８を通じてコンピュータ１３１２に論理的に接続され、通信接続１３５０を介して物理的に接続される。ネットワークインターフェイス１３４８は、ローカルエリアネットワーク（ＬＡＮ）およびワイドエリアネットワーク（ＷＡＮ）などの通信ネットワークを含む。ＬＡＮ技術には、Ｆｉｂｅｒ Ｄｉｓｔｒｉｂｕｔｅｄ Ｄａｔａ Ｉｎｔｅｒｆａｃｅ（ＦＤＤＩ）、Ｃｏｐｐｅｒ Ｄｉｓｔｒｉｂｕｔｅｄ Ｄａｔａ Ｉｎｔｅｒｆａｃｅ（ＣＤＤＩ）、Ｅｔｈｅｒｎｅｔ（登録商標）／ＩＥＥＥ １３０２．３、Ｔｏｋｅｎ Ｒｉｎｇ／ＩＥＥＥ １３０２．５などがある。ＷＡＮ技術には、２地点間接続リンク、統合デジタル通信網（ＩＳＤＮ）などの回線交換ネットワークとその変種、パケット交換ネットワーク、およびデジタル加入者回線（ＤＳＬ）などがある。

【０１０８】

通信接続１３５０とは、ネットワークインターフェイス１３４８をバス１３１８に接続するために使用されるハードウェア／ソフトウェアのことである。通信接続１３５０はわかりやすくするためにコンピュータ１３１２内に示されているが、コンピュータ１３１２の外部にあってもかまわない。ネットワークインターフェイス１３４８の接続に必要なハードウェア／ソフトウェアには、例えば、通常の電話程度のモデム、ケーブルモデム、およびＤＳＬモデムを含むモデム、ＩＳＤＮアダプタ、およびＥｔｈｅｒｎｅｔ（登録商標）カードなどの内部および外部技術がある。

【０１０９】

上述の内容には、本発明の実施例が含まれる。もちろん、本発明を説明するためにコンポーネントまたは方法の考えられるすべての組合せを説明することは不可能であるが、当業者であれば、本発明の他の多くの組合せおよび置換が可能であることは理解できるであろう。したがって、本発明は、請求項の精神と範囲に収まるそのようなすべての改変、修正、およびバリエーションを包含するものとする。さらに、「含む」という言い回しを詳細な説明または請求項で使用している範囲において、このような用語は、「備える、含む」という用語と同様の使い方をし、これは使用した場合に請求項の中で暫定的用語と解釈する。

【図面の簡単な説明】

【図１】本発明の一態様による迷惑電子メールを検出するシステムのブロック図である。

【図２】本発明の一態様による迷惑電子メールを検出するシステムのブロック図である。

【図３】本発明の一態様による迷惑電子メールを検出するシステムのブロック図である。

【図４】本発明の一態様による迷惑電子メールを検出するシステムのブロック図である。

【図５】本発明の一態様による迷惑電子メールを検出するシステムのブロック図である。

【図６】本発明の一態様による迷惑電子メールを検出するシステムのブロック図である。

【図７】本発明の一態様によるチャレンジに応答するシステムのブロック図である。

【図８】本発明の一態様による迷惑電子メールを検出する方法を例示する流れ図である。

【図９】図８の方法を例示する流れ図である。

【図１０】本発明の一態様によりチャレンジに応答するための方法を例示する流れ図である。

【図１１】本発明の一態様によりチャレンジに応答するための方法を例示する流れ図である。

【図１２】本発明の一態様による複数のチャレンジに応答するユーザインターフェイス例の図である。

【図１３】本発明が機能すると思われる動作環境例を示す図である。

【符号の説明】

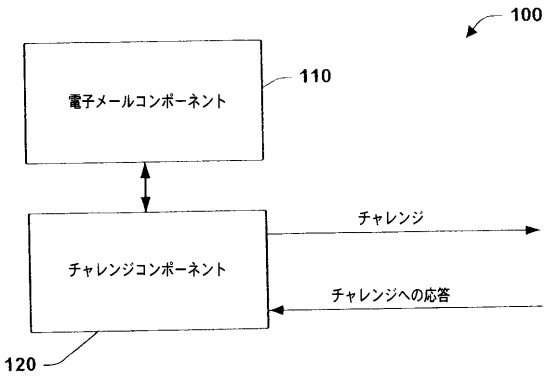
１００　システム

１１０　電子メールコンポーネント

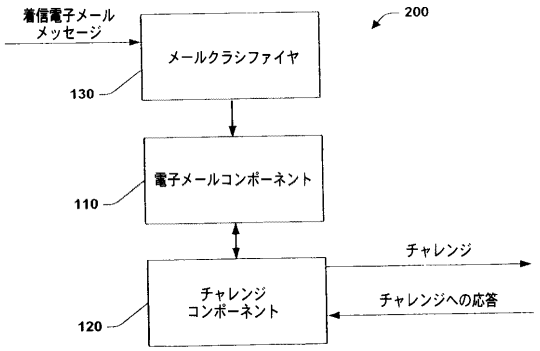
１２０　チャレンジコンポーネント

１３０　メールクラシファイヤ
２００　システム
３００　システム
３１０　メールクラシファイヤ
３２０　チャレンジコンポーネント
３３０　スパムフォルダ
３４０　正当な電子メールフォルダ
３５０　正当な電子メール送信者記憶領域
３６０　スパム送信者記憶領域
４００　システム
５００　システム
５１０　メールクラシファイヤ
５２０　チャレンジコンポーネント
５３０　スパムフォルダ
５４０　疑わしいスパムフォルダ
５５０　正当な電子メールフォルダ
５６０　正当な電子メール送信者記憶領域
５７０　スパム送信者記憶領域
６００　システム
６６０　正当な電子メール送信者記憶領域
７００　システム
７１０　チャレンジチャレンジ受信コンポーネント
７２０　チャレンジプロセッサコンポーネント
７３０　チャレンジ応答コンポーネント
８００　方法
１０００　方法
１１００　方法
１３１０　動作環境
１３１２　コンピュータ
１３１４　処理装置
１３１６　システムメモリ
１３１８　システムバス
１３２０　揮発性メモリ
１３２２　不揮発性メモリ
１３２４　ディスク記憶装置
１３２８　オペレーティングシステム
１３３６　入力デバイス
１３３８　インターフェイスポート
１３４０　出力デバイス
１３４２　出力アダプタ
１３４４　リモートコンピュータ
１３４６　メモリ記憶装置
１３４８　ネットワークインターフェイス
１３５０　通信接続

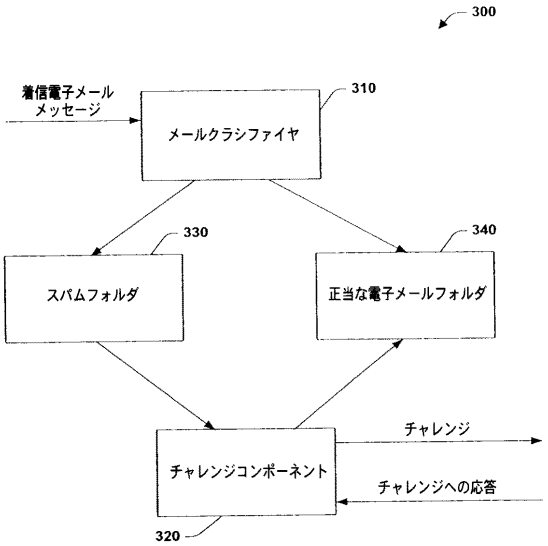
【図１】


100
電子メールコンポーネント
110
チャレンジコンポーネント
チャレンジ
チャレンジへの応答
120

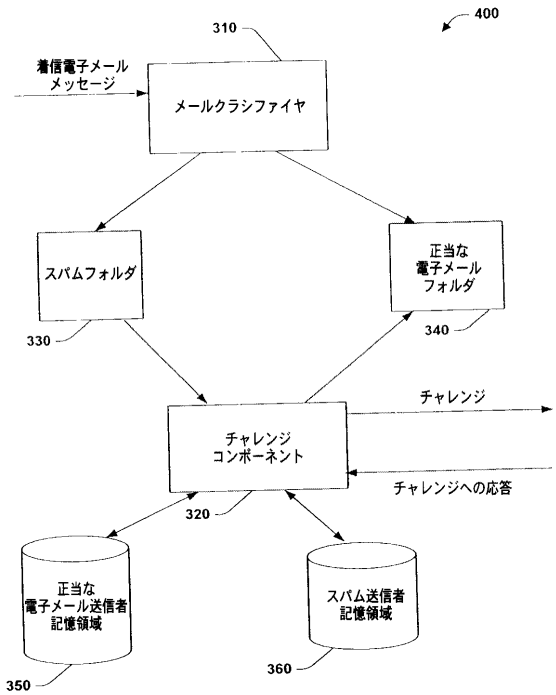
【図２】


着信電子メール
メッセージ
200
メールクラシファイヤ
130
電子メールコンポーネント
110
チャレンジ
チャレンジ
コンポーネント
チャレンジへの応答
120

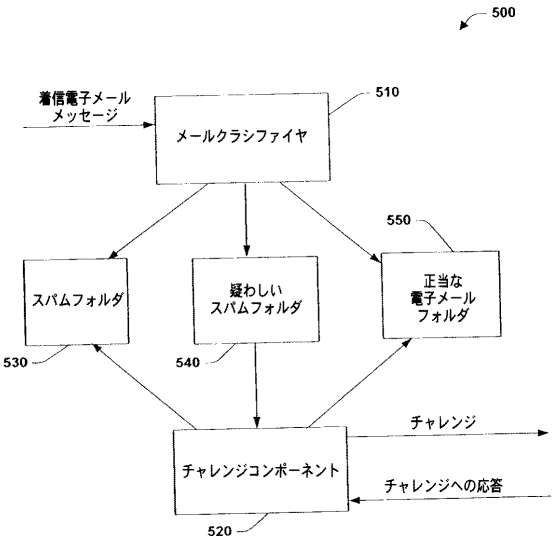
【図３】


300
着信電子メール
メッセージ
310
メールクラシファイヤ
330
340
スパムフォルダ
正当な電子メールフォルダ
チャレンジ
チャレンジコンポーネント
チャレンジへの応答
320

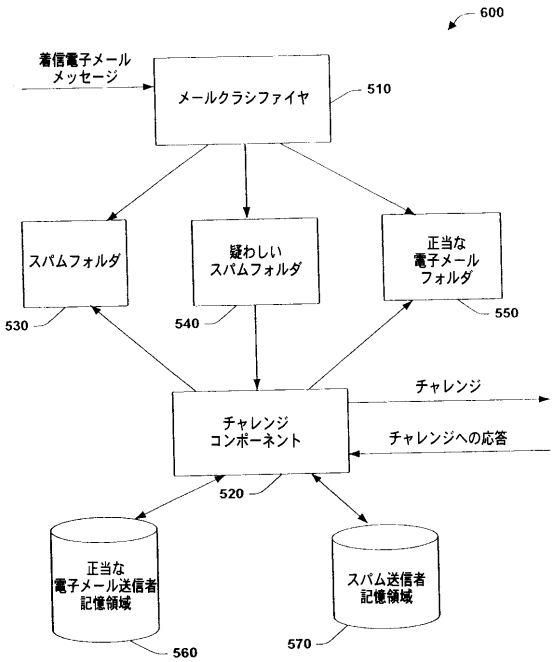
【図４】


400
310
着信電子メール
メッセージ
メールクラシファイヤ
スパムフォルダ
正当な
電子メール
フォルダ
330
340
チャレンジ
チャレンジ
コンポーネント
チャレンジへの応答
320
正当な
電子メール送信者
記憶領域
スパム送信者
記憶領域
350
360

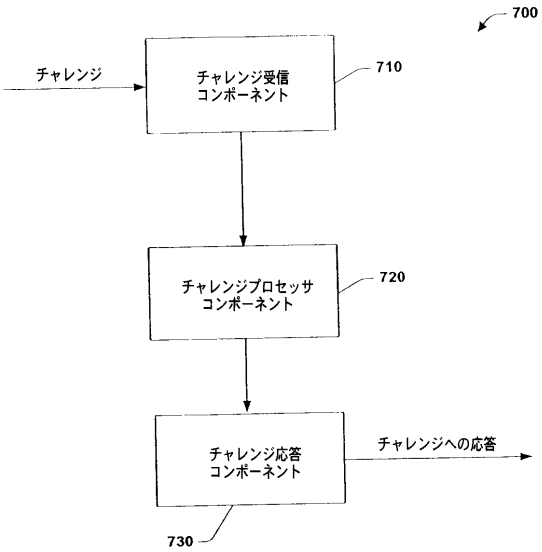
【図５】


500
着信電子メール
メッセージ
510
メールクラシファイヤ
550
スパムフォルダ
疑わしい
スパムフォルダ
正当な
電子メール
フォルダ
530
540
チャレンジ
チャレンジコンポーネント
チャレンジへの応答
520

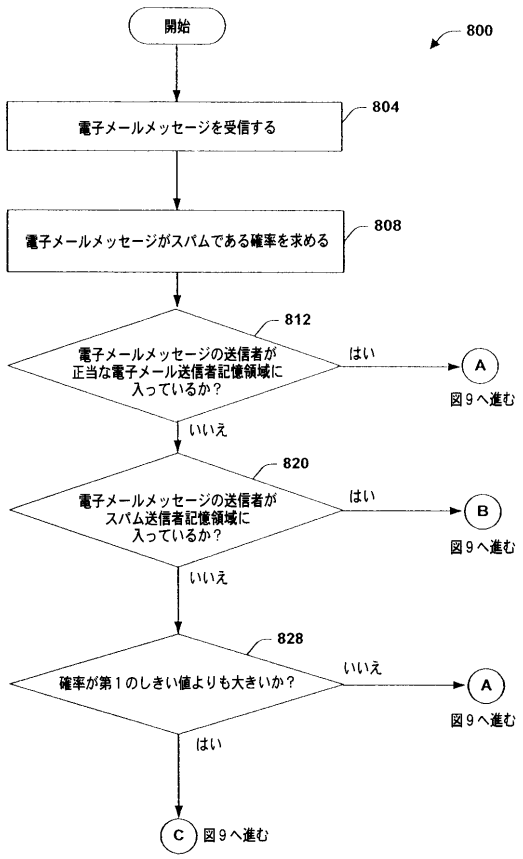
【図６】


600
着信電子メール
メッセージ
メールクラシファイヤ
510
スパムフォルダ
530
疑わしい
スパムフォルダ
540
正当な
電子メール
フォルダ
550
チャレンジ
コンポーネント
520
チャレンジ
チャレンジへの応答
正当な
電子メール送信者
記憶領域
560
スパム送信者
記憶領域
570

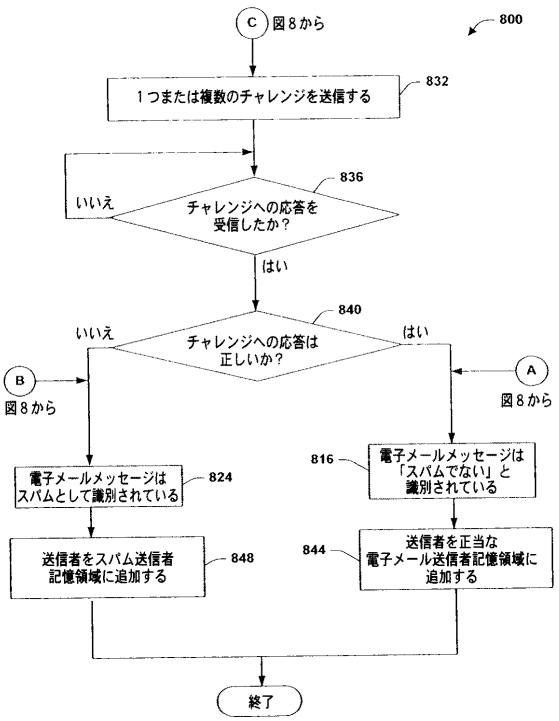
【図７】


700
チャレンジ
チャレンジ受信
コンポーネント
710
チャレンジプロセッサ
コンポーネント
720
チャレンジ応答
コンポーネント
チャレンジへの応答
730

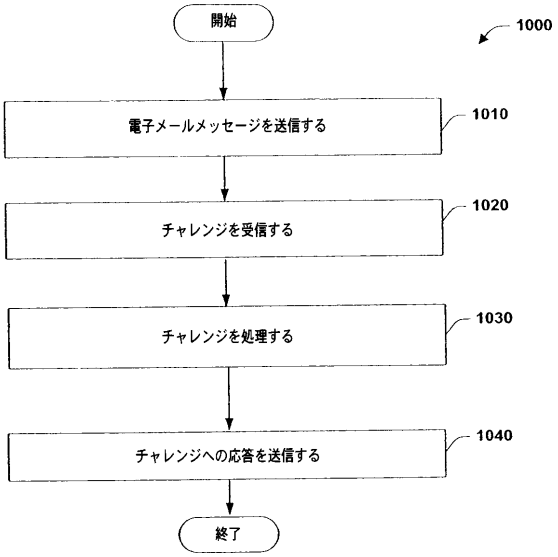
【図８】


開始
800
電子メールメッセージを受信する
804
電子メールメッセージがスパムである確率を求める
808
812
電子メールメッセージの送信者が
正当な電子メール送信者記憶領域に
入っているか？
はい
A
図９へ進む
いいえ
820
電子メールメッセージの送信者が
スパム送信者記憶領域に
入っているか？
はい
B
図９へ進む
いいえ
828
確率が第１のしきい値よりも大きいか？
いいえ
A
図９へ進む
はい
C
図９へ進む

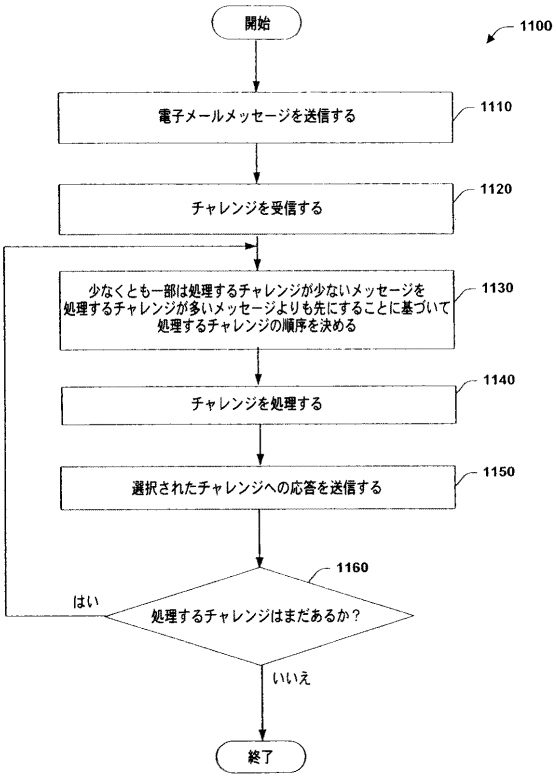
【図９】


C
図８から
800
１つまたは複数のチャレンジを送信する
832
836
いいえ
チャレンジへの応答を
受信したか？
はい
840
いいえ
チャレンジへの応答は
正しいか？
はい
B
図８から
A
図８から
電子メールメッセージは
スパムとして識別されている
824
816
電子メールメッセージは
「スパムでない」と
識別されている
送信者をスパム送信者
記憶領域に追加する
848
844
送信者を正当な
電子メール送信者記憶領域に
追加する
終了

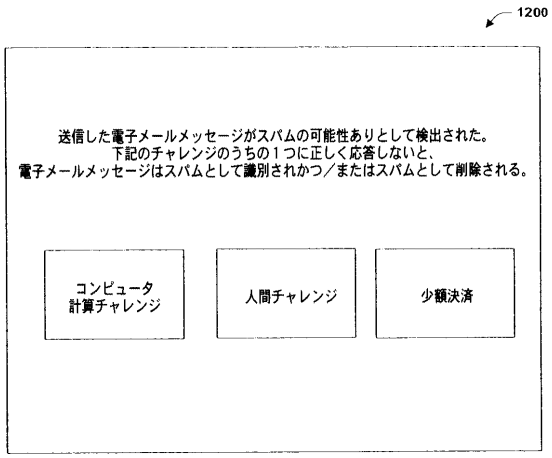
【図１０】



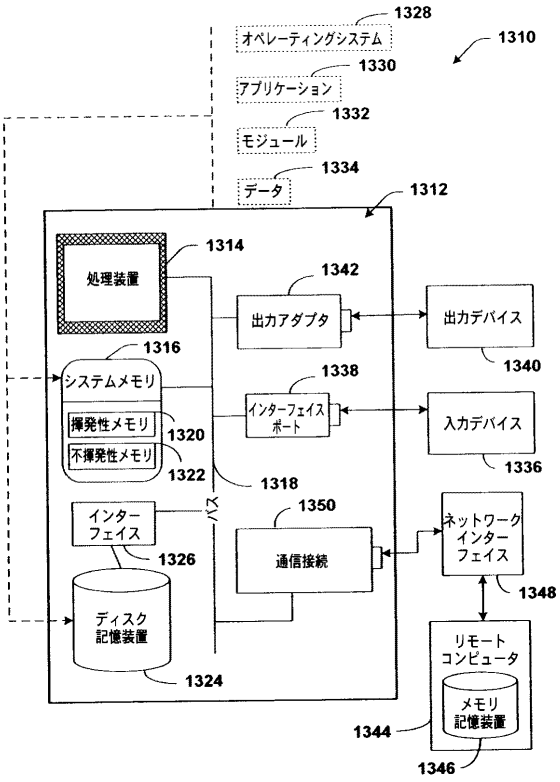
【図１１】



【図１２】



【図１３】



フロントページの続き

(72)発明者　ロバート　エル．ランスウェイト
アメリカ合衆国　９８０２４　ワシントン州　フォール　シティ　２８７　アベニュー　サウスイースト　４１４８

審査官　高瀬　勤

(56)参考文献　特開２００２－１４９６１１（ＪＰ，Ａ）
国際公開第０１／０４６８７２（WO，Ａ１）
国際公開第０２／０３００５４（WO，Ａ１）
国際公開第０２／０２３３９０（WO，Ａ１）
特開２０００－１６３３４１（ＪＰ，Ａ）
特開２００２－１６４８８７（ＪＰ，Ａ）
川又　英紀，企業が始めた「インターネットの利用制限」，日経コンピュータ，日本，日経ＢＰ社，１９９９年　5月１０日，no.469，p87-91

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F　13/00
G06F　21/00
JSTPlus(JDreamII)