(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4839318号
(P4839318)
(45)発行日　平成23年12月21日(2011.12.21)　(24)登録日　平成23年10月7日(2011.10.7)

(51)Int.Cl.　　F I
H04L 12/66 (2006.01)　　H04L 12/66　B
G06F 13/00 (2006.01)　　G06F 13/00　610Q

請求項の数 10　(全 28 頁)

(21)出願番号	特願2007-540073 (P2007-540073)
(86)(22)出願日	平成17年11月4日 (2005.11.4)
(65)公表番号	特表2008-519532 (P2008-519532A)
(43)公表日	平成20年6月5日 (2008.6.5)
(86)国際出願番号	PCT/US2005/039978
(87)国際公開番号	WO2006/052736
(87)国際公開日	平成18年5月18日 (2006.5.18)
審査請求日	平成20年10月20日 (2008.10.20)
(31)優先権主張番号	60/625,507
(32)優先日	平成16年11月5日 (2004.11.5)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	11/142,943
(32)優先日	平成17年6月2日 (2005.6.2)
(33)優先権主張国	米国 (US)

(73)特許権者　507312747
セキュアー　コンピューティング　コーポレイション
アメリカ合衆国　ミネソタ　５５１０８，セント　ポール，　エナジー　パーク　ドライブ　２３４０
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】メッセージプロファイリングシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
メッセージングエンティティに対する評判を指定するための１つ以上のデータプロセッサ上で動作する方法であって、該方法は、
メッセージングエンティティの通信に関連する１つ以上の特性を識別するデータを受信することと、
評判が良い分類と評判が良くない分類とを区別することに使用される一セットの判定基準内の各判定基準に対して、
１つ以上のデータプロセッサにより、その判定基準が該メッセージングエンティティに適用するかどうかを決定すること、
該１つ以上のデータプロセッサにより、その判定基準が該メッセージングエンティティに適用することを決定したことに応答して、該メッセージングエンティティが評判が良くないメッセージングエンティティである第１の条件付き確率を決定すること、および
該１つ以上のデータプロセッサにより、その判定基準が該メッセージングエンティティに適用することを決定したことに応答して、該メッセージングエンティティが評判が良いメッセージングエンティティである第２の条件付き確率を決定することと、
該１つ以上のデータプロセッサにより、該メッセージングエンティティが評判が良くないメッセージングエンティティであることを示す第１の確率を決定することであって、該第１の確率は、該第１の条件付き確率の積から決定される、ことと、
該１つ以上のデータプロセッサにより、該メッセージングエンティティが評判が良いメ

ッセージングエンティティであることを示す第２の確率を決定することであって、該第２の確率は、該第２の条件付き確率の積から決定される、ことと、
該１つ以上のデータプロセッサにより、該第１の確率および該第２の確率から評判スコアを決定することであって、該決定された評判スコアは、該メッセージングエンティティの評判を示す、ことと
を含み、
該決定された評判スコアは、該メッセージングエンティティに関連する通信に対して、どの行動がとられるべきかを決定することに使用される、方法。
【請求項２】
請求項１に記載の方法であって、前記決定された評判スコアは、トランスミッションのフィルタリングに使用する１つ以上のコンピュータシステムに分配される、方法。
【請求項３】
請求項１に記載の方法であって、前記決定された評判スコアは、トランスミッションのフィルタリングに使用するプログラムにローカルに分配される、方法。
【請求項４】
請求項１に記載の方法であって、前記評判スコアは、前記メッセージングエンティティの特性および挙動に基づいてメッセージングエンティティに指定された数値、テキストまたはカテゴリの評判を含み、該数値の評判は、評判が良い分類と評判が良くない分類との間の連続的なスペクトルで変動する、方法。
【請求項５】
請求項１に記載の方法であって、評判が指定されるメッセージングエンティティのタイプは、電子メッセージを送信する組織、コンピュータまたは個別のユーザを表すドメインネーム、ＩＰアドレス、電話番号、個別の電子アドレスまたは個別のユーザ名である、方法。
【請求項６】
請求項１に記載の方法であって、各メッセージングエンティティの評判は、３２ビットの付点のついたデシマルＩＰアドレス形式でエンコードされ、該方法は、
メッセージングエンティティの世界において全てのメッセージングエンティティの該評判を含むドメインネームサーバ（ＤＮＳ）ゾーンを作り出すことと、
メッセージングエンティティの評判を、ＤＮＳプロトコルを通じて、１つ以上のコンピュータシステムに分配することであって、該１つ以上のコンピュータシステムは、それらの動作において該評判を利用する、ことと
をさらに含む、方法。
【請求項７】
請求項１に記載の方法であって、前記一セットの判定基準は、グループ：
平均のスパムプロファイラスコアと、リバースドメインネームサーバのルックアップフェイラと、１つ以上のリアルタイムブラックリスト（ＲＢＬ）におけるメンバシップと、メール量と、メールバースティネスと、メールブレドスと、地理学的な位置と、マルウェアの活動と、アドレスのタイプと、スパムを送信すると識別される多数のインターネットプロトコルアドレスを含むクラスレスドメイン間ルーティング（ＣＩＤＲ）ブロックと、ユーザのクレームの割合と、ハニーポット発見の割合と、トランスミッションの挙動の法律、規則および確立した標準に従うと識別された、送達不可能なトランスミッションの割合と、動作の連続性と、レシピエントの需要への応答と、これらの組み合わせ
から選択された判定基準である、方法。
【請求項８】
請求項１に記載の方法であって、前記メッセージングエンティティの評判を、
【数１】

$$IP = 172.\left(\frac{rep - |rep|}{2 \times rep}\right).(|rep| div 256).(|rep| \bmod 256).$$

を含む関数に従って、３２ビットの付点のついたデシマルＩＰアドレスでエンコードすることをさらに含む、方法。
【請求項９】
請求項１に記載の方法であって、評判が良いおよび評判が良くないという分類は、望まれないトランスミッション、または正当な通信を送信するためのＩＰアドレスの傾向に関連する、方法。
【請求項１０】
命令がエンコードされたコンピュータ読み取り可能な記憶デバイスであって、
該命令は、１つ以上のデータ処理デバイスに、
メッセージングエンティティの通信に関連する１つ以上の特性を識別するデータを受信することと、
評判が良い分類と評判が良くない分類とを区別することに使用される一セットの判定基準内の各判定基準に対して、
その判定基準が該メッセージングエンティティに適用するかどうかを決定すること、
その判定基準が該メッセージングエンティティに適用することを決定したことに応答して、該メッセージングエンティティが評判が良くないメッセージングエンティティである第１の条件付き確率を決定すること、および
その判定基準が該メッセージングエンティティに適用することを決定したことに応答して、該メッセージングエンティティが評判が良いメッセージングエンティティである第２の条件付き確率を決定することと、
該メッセージングエンティティが評判が良くないメッセージングエンティティであることを示す第１の確率を決定することであって、該第１の確率は、該第１の条件付き確率の積から決定される、ことと、
該メッセージングエンティティが評判が良いメッセージングエンティティであることを示す第２の確率を決定することであって、該第２の確率は、該第２の条件付き確率の積から決定される、ことと、
該第１の確率および該第２の確率から評判スコアを決定することであって、該決定された評判スコアは、該メッセージングエンティティの評判を示す、ことと
を含む動作を実行させ、
該決定された評判スコアは、該メッセージングエンティティに関連する通信に対して、どの行動がとられるべきかを決定することに使用される、コンピュータ読み取り可能な記憶デバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
この文書は通信を処理するためのシステムおよび方法に広く関連し、特に通信をフィルタリングするためのシステムおよび方法に関連している。
【背景技術】
【０００２】
反スパム（ａｎｔｉ－ｓｐａｍ）産業においては、スパム送信者（ｓｐａｍｍｅｒ）は、スパムフィルタによる検出を回避するための種々の独創的な手段を使用する。利用可能な反スパムシステムは、フェイルオープン（ｆａｉｌ－ｏｐｅｎ）システムを含み、フェイルオープンシステムにおいて、全ての入力メッセージがスパムに対するフィルタをかけられる。しかしながら、これらのシステムは、正当またはスパムとして正しく分類されるメッセージにおいては、非効率および不正確であり得る。
【発明の開示】
【課題を解決するための手段】
【０００３】
本明細書で開示される教示に従って、方法およびシステムが、メッセージングエンティティに評判を指定する１つ以上のデータプロセッサ上に動作を提供される。例えば、方法

およびシステムは、メッセージングエンティティの通信に関連する１つ以上の特性を識別するデータを受信することと、受信された識別データに基づいて評判を決定することとを含み、決定された評判スコアは、メッセージングエンティティの評判を指示し、決定された評判スコアは、メッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【０００４】

別の例として、トランスミッションセンダの評判スコアを利用するトランスミッションフィルタリングを行うシステムおよび方法が、提供される。システムおよび方法は、センダからのトランスミッションについて少なくとも１つの特性を識別することと、トランスミッション特性を含む評判システムに対してリアルタイムの照会（ｑｕｅｒｙ）を行うことと、トランスミッションに関連する評判を表すスコアを受信することと、センダからのトランスミッションに、センダの評判のスコアの範囲に対応する行動を実行することとを含み得る。

【０００５】

別の例として、トランスミッションのセンダの評判スコアを利用するトランスミッションのグループのフィルタリングを行うためのシステムおよび方法が提供される。例えば、システムおよび方法は、コンテンツの類似性またはトランスミッションセンダの挙動における類似性に基づいて複数のトランスミッションを共にグルーピングすることと、グルーピングにおける各トランスミッションについて少なくとも１つの特性を識別することと、評判システムに対して照会を行い、各センダの評判を表すスコアを受信することと、グループにおける評判が良いセンダおよび評判が良くないセンダのパーセンテージに基づいてトランスミッションのグループを分類することと、を含み得る。

【０００６】

別の例として、訓練可能なトランスミッションのセットにおいて、トランスミッションのセンダの評判スコアを利用するフィルタリングシステムの調整および訓練を行うためのシステムおよび方法が提供される。例えば、方法はセンダからのトランスミッションについて少なくとも１つの特性を識別することと、評判システムに対して照会を行い、センダの評判を表すスコアを受信することと、センダの評判スコアが分類される範囲に基づいて複数のカテゴリにトランスミッションを分類することと、フィルタリングシステムの最適化のために使用されるべき別のフィルタリングシステムのトレーナにトランスミッションおよびトランスミッションの分類カテゴリを受け渡すことと、を含み得る。

【０００７】

別の例として、メッセージングエンティティからの通信を分類するために１つ以上のデータプロセッサ上で動作するシステムおよび方法が提供される。例えば、システムおよび方法は、メッセージングエンティティからの通信を受信することと、通信を分類するために複数のメッセージ分類手法を使用することと、メッセージプロファイルスコアを生成するためにメッセージ分類出力を組み合わせることとを含み得、メッセージプロファイルスコアは、メッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【０００８】

別の例として、このようなシステムおよび方法は、センダからのトランスミッションについて少なくとも１つの特性を識別することと、評判システムに対して照会を行い、センダの評判を表すスコアを受信することと、センダの評判スコアが分類される範囲に基づいて複数のカテゴリにトランスミッションを分類することと、フィルタリングシステムの最適化のために使用されるべき別のフィルタリングシステムのトレーナにトランスミッションおよびトランスミッションの分類カテゴリを受け渡すことと、を含み得る。

【０００９】

別の例として、このようなシステムおよび方法は、メッセージングエンティティからの通信を受信することと、通信を分類するために複数のメッセージ分類手法を使用することと、メッセージプロファイルスコアを生成するためにメッセージ分類出力を組み合わせる

こととを含み得、メッセージプロファイルスコアは、メッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【００１０】

本明細書で開示される教示に従って、方法およびシステムは、メッセージングエンティティからの通信を分類する１つ以上のデータプロセッサ上に動作を提供される。例えば、システムおよび方法は、複数のメッセージ分類手法を含み得、手法は、メッセージングエンティティから受信される通信を分類するように構成される。システムおよび方法は、メッセージプロファイルスコアを生成するためにメッセージ分類出力を組み合わせるように構成されるメッセージプロファイリング論理をさらに含み得、メッセージプロファイルスコアは、メッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【００１１】

別の例として、方法およびシステムは、メッセージングエンティティから送達された通信を受信することを含み得る。複数のメッセージ分類手法が通信を分類するために使用される。メッセージ分類手法は信頼値に関連し、信頼値はメッセージ分類手法からメッセージ分類出力を生成することに使用される。メッセージ分類出力は、メッセージプロファイルスコアを生成するために組み合わせられる。メッセージプロファイルスコアはメッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【００１２】

別の例として、システムおよび方法は、複数のメッセージ分類手法を利用し得、複数のメッセージ分類手法は、メッセージングエンティティから受信された通信を分類するように構成される。メッセージプロファイリング論理は、メッセージプロファイルスコアを生成するためにメッセージ分類出力を組み合わせるように構成され得る。メッセージプロファイルスコアは、メッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【００１３】

別の例として、システムおよび方法は、１つ以上のメッセージ分類手法による使用のためのメッセージ分類パラメータの調整に使用され得る。複数の通信である、または複数のデータを表す、複数の入力データが受信される（例えば、入力論理または処理命令を介して）。チューナプログラムは、メッセージ分類手法に関連するメッセージ分類パラメータを調整するために使用される。通信はメッセージングエンティティから受信される。調整されたメッセージ分類パラメータは、通信を分類するために複数のメッセージ分類手法によって使用される。複数のメッセージ分類手法からのメッセージ分類出力は、メッセージプロファイルスコアを生成するために組み合わせられる。メッセージプロファイルスコアは、メッセージングエンティティに関連する通信に対してどの行動がとられるべきかを決定することに使用される。

【発明を実施するための最良の形態】

【００１４】

（詳細な説明）

図１は、３０において、ネットワーク４０上で受信されるトランスミッションを扱うためのシステムを描いている。トランスミッションは多くの異なるタイプの通信（例えば、１つ以上のメッセージングエンティティ（ｍｅｓｓａｇｉｎｇ　ｅｎｔｉｔｙ）５０から送られた電子メール（ｅ－ｍａｉｌ）メッセージ）であり得る。システム３０は、メッセージングエンティティ（例えば、メッセージングエンティティ５２）に対して分類を指定し、メッセージングエンティティに指定された分類に基づいて、メッセージングエンティティの通信に関して行動がとられる。

【００１５】

システム３０は、メッセージングエンティティ５０からの処理通信を支援するために、フィルタリングシステム６０、および評判システム（ｒｅｐｕｔａｔｉｏｎ　ｓｙｓｔｅ

ｍ）７０を使用する。フィルタリングシステム６０は、どんなフィルタリング行動（もしあるのならば）がメッセージングエンティティの通信上でなされるかの決定を支援するために、評判システム７０を使用する。例えば、通信は評判が良い供給源からであると決定され得、従って通信はフィルタされない。

【００１６】

フィルタリングシステム６０は、６２において、受信された通信に関連する１つ以上のメッセージ特性を識別し、評判システム７０に対して識別情報（ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｉｎｆｏｒｍａｔｉｏｎ）を提供する。評判システム７０は、識別されたメッセージ特性が特定の質を示す確率を計算することにより、評判を評価する。全体としての評判スコアは、計算された確率に基づいて決定され、フィルタリングシステム６０に提供される。

【００１７】

フィルタリングシステム６０は、センダ（ｓｅｎｄｅｒ）の通信のためにどんな行動がとられるかを決定するために、６４において評判スコアを調査する（例えば、通信トランスミッションが、メッセージ受信システム８０内に位置される、通信の指定されたレシピエント（ｒｅｃｉｐｉｅｎｔ）に届けられるかどうか）。フィルタリングシステム６０は、通信が、評判システム７０によって提供されたスコアを付けられた評判の全体に、または一部に基づいて扱われると決定し得る。実例として、通信は、評判が良くない（ｎｏｎ－ｒｅｐｕｔａｂｌｅ）センダからであると決定され得、結果として通信はＳｐａｍとして扱われる（例えば、削除されたり、隔離（ｑｕａｒａｎｔｉｎｅ）されたり、など）。

【００１８】

評判システムは、フィルタリングシステムを支援するために、多くの異なる方法で構成され得る。例えば、評判システム７０は、当面の状況に依存して、フィルタリングシステム６０に対して外部、または内部に位置され得る。別の例として、図２は、このような、８２において示されているようなセンダのアイデンティティとしてのメッセージ特性識別情報に基づいて、評判スコアを計算するように構成される評判システム７０を描いている。他のメッセージ特性が、センダのアイデンティティの代わりに、またはセンダのアイデンティティに加えて使用され得ることが理解される。さらに、トランスミッションは、多くの異なるタイプのメッセージングエンティティからであり得る（例えば、ドメインネーム、ＩＰアドレス、電話番号、または個別の電子アドレス、組織を代表するユーザ名、コンピュータ、または電子メッセージを送信する個別のユーザ）。例えば、評判が良い、および評判が良くないという、生成された分類は、望まれないトランスミッション、または正当な通信を送信するためのＩＰアドレスの傾向に基づき得る。

【００１９】

システムの構成９０はまた、図２に示され、バイナリのテスト可能な判定基準９２のセットを識別することにより確立され得、判定基準９２は、良いセンダと悪いセンダとの間の強いディスクリミネータと思われる。Ｐ（ＮＲ｜C_i）は、センダが質／判定基準C_iに従う場合には、上記センダは評判が良くないという確率として定義され得、Ｐ（Ｒ｜C_i）は、センダが質／判定基準C_iに従う場合には、上記センダが評判である関数として定義され得る。

【００２０】

質／判定基準C_iの各々に対し、周期的な（例えば、一日の、一週間の、一月の、など）サンプリング演習が、Ｐ（ＮＲ｜C_i）の再計算をするために行われ得る。サンプリング演習は、質／判定基準C_iが真であることが既知のセンダＮのランダムサンプルセットＳを選択することを含み得る。サンプル中のセンダは、次いで以下のセットの内の１つにソートされる：評判が良い（Ｒ）、評判が良くない（ＮＲ）、または未知（Ｕ）。N_Rは、評判が良いセンダであるサンプルにおけるセンダ数であり、N_{NR}は、評判が良くないセンダのセンダ数、などである。次いで、Ｐ（ＮＲ｜C_i）およびＰ（Ｒ｜C_i）は、式：

【００２１】

【数５】

$$P(NR \mid C_i) = \frac{N_{NR}}{N}$$

$$P(R \mid C_i) = \frac{N_R}{N}$$

を用いて推定される。この目的において、Ｎ＝３０は、各々の質／判定基準Ｃ$_i$に対してＰ（ＮＲ｜Ｃ$_i$）およびＰ（Ｒ｜Ｃ$_i$）の正確な推定を達成するためには大きすぎるサンプルサイズであることが決定される。

【００２２】

全ての判定基準に対し、Ｐ（ＮＲ｜Ｃ$_i$）およびＰ（Ｒ｜Ｃ$_i$）を計算した後に、算出された確率は、評判スペースにおける各センダの、評判が良くない確率の総計Ｐ$_{NR}$　９４、および評判が良いセンダの確率の総計Ｐ$_R$　９６を計算されるために使用される。これらの確率は式：

【００２３】

【数６】

$$P_{NR} = \left(1 - \prod_{i=1}^{N} \begin{cases} 1 - P(NR \mid C_i) & \text{判定基準iを適用した場合} \\ 1 & \text{それ以外の場合} \end{cases}\right)^{(\#\text{適用する判定基準の})}$$

$$P_R = \left(1 - \prod_{i=1}^{N} \begin{cases} 1 - P(R \mid C_i) & \text{判定基準iを適用した場合} \\ 1 & \text{それ以外の場合} \end{cases}\right)^{(\#\text{適用する判定基準の})}$$

を用いて計算され得る。実験においては、上記の式は広範囲の入力判定基準の組み合わせに対して非常に良い挙動を見せ、実際には、それらの挙動は、入力判定基準の「評判が良くない」および「評判が良い」挙動の条件付き確率の単純な（ｎａｉｖｅ）結合を正確に算出するための式の挙動に類似するように見える。

【００２４】

各センダに対して、Ｐ$_{NR}$およびＰ$_R$を計算した後に、評判スコアは、そのセンダに対して以下の評判関数：

【００２５】

【数７】

$$f(P_{NR}, P_R) = (c_1 + c_2 P_{NR} + c_2 P_R + c_3 P_{NR}^2 + c_3 P_R^2 + c_4 P_{NR} P_R + c_5 P_{NR}^3 + c_5 P_R^3 + c_6 P_{NR} P_R^2 + c_6 P_{NR}^2 P_R)((P_{NR} - P_R)^3 + c_7 (P_{NR} - P_R))$$

ここで

$$c_1 = 86.50$$
$$c_2 = -193.45$$
$$c_3 = -35.19$$
$$c_4 = 581.09$$
$$c_5 = 234.81$$
$$c_6 = -233.18$$
$$c_7 = 0.51$$

を用いて計算される。異なる関数が、評判スコアのデタミネータ９８として振舞い、関数の表現に加えて、多くの異なる形式で表現され得ることが理解される。実例として、図３は、１００において評判スコアを決定するための表形式を描いている。表は、Ｐ$_{NR}$およ

びP_Rに基づいて、それらが０．０～１．０の間で変動する場合に、上記の関数により生成される評判スコアを示している。例えば、１１０に示されているように、５３という評判スコアはP_{NR}＝０．９およびP_R＝０．２の組み合わせにおいて取得される。この評判スコアは、センダが評判が良いと考慮されない比較的高い指標である。０という評判スコアは、P_{NR}およびP_Rが同一である場合に取得される（例えば、１２０において示されるように、P_{NR}＝０．７およびP_R＝０．７の場合に、評判スコアが０になる）。評判スコアは、P_RがP_{NR}よりも大きい場合に決定される、センダが比較的評判が良いことを指示するための負の値を有し得る。例えば、１３０に示されるように、P_{NR}＝０．５およびP_R＝０．８の場合には、評判スコアは－１２である。

【００２６】

評判スコアは図４の１５０に描かれるように、図式的に示され得る。グラフ１５０は、P_{NR}およびP_Rの値に基づいて、上記の関数より生成された。図４は、項P_{NR}、およびP_Rが、各々０．０～１．０の間で変動する確率として、各々ノンスパム性（ｈａｍｍｉｎｅｓｓ）の確率、およびスパム性の（ｓｐａｍｍｉｎｅｓｓ）の確率として使用されるという点で、Ｓｐａｍのコンテキストにおける評判スコアの決定を図示している。

【００２７】

これらの例において示されるように、評判スコアは、通信の特性（例えば、メッセージングエンティティ特性）、および／またはメッセージングエンティティの挙動に基づいてメッセージングエンティティを指定される数値の評判（ｎｕｍｅｒｉｃ　ｒｅｐｕｔａｔｉｏｎ）であり得る。数値の評判は、評判が良いという分類の連続スペクトルと、評判が良くないという分類の連続スペクトルとの間で変動（ｆｌｕｃｔｕａｔｅ）し得る。しかしながら、評判は、例えば、テキストのカテゴリ、または複数のレベルのテキストのカテゴリによって、非数値のもの（ｎｏｎ－ｎｕｍｅｒｉｃ）であり得る。

【００２８】

図５は、動作シナリオを描いており、評判システムは、評判スコアを生成するためにフィルタリングシステムにより使用される。この動作シナリオにおいては、評判スコアは、入力データのセットから、特定のセンダ（例えば、ＩＰアドレス、ドメインネーム、電話番号、住所など）において算出される。図５を参照すると、データは、センダにおける、評判が良くない確率、および評判が良い確率を計算するために必要なステップ２００において収集される。データは、次いで、ステップ２１０において統合され、ステップ２２０において確率の計算に使用される。これは、多種の選択された判定基準において、センダに対する評判が良くない確率、および評判が良い確率を決定することを含む。評判が良くない確率の総計、および評判が良い確率の総計は、次いで各センダに対して計算される。

【００２９】

各センダに対し、評判が良くない確率の総計、および評判が良い確率の総計を計算した後に、評判スコアは、評判関数を用いるそのセンダに対し、２３０で計算される。ステップ２４０において、センダの評判スコアは、センダに関連する通信を評価するために、ローカルに、および／または１つ以上のシステムに分配される。実例として、評判スコアは、フィルタリングシステムに分配され得る。評判スコアによって、フィルタリングシステムは、センダの評判スコアが分類される範囲に基づいて、トランスミッション上に作用するように選ばれ得る。評判が悪い（ｕｎｒｅｐｕｔａｂｌｅ）センダに対しては、フィルタリングシステムは、トランスミッションをドロップすることを選び得（例えば、静かに）、それが隔離領域に保存することを選び得、または疑わしいとしてトランスミッションにフラグを立てることを選び得る。さらに、フィルタシステムは、特定の期間におけるこのセンダからの全ての将来のトランスミッションに、評判システムに作成させるために新たなルックアップ照会（ｌｏｏｋｕｐ　ｑｕｅｒｙ）を必要とすることなく、このような行動を適用するために選ばれ得る。評判が良いセンダに対し、フィルタリングシステムは、トランスミッションが、フィルタリングシステムにおける、有意な、処理のオーバヘッド、ネットワークのオーバヘッド、または記憶のオーバヘッドを引き起こす、全ての、またはあるフィルタリング手法をバイパスさせるために、トランスミッションに、行動を同

様に適用する。

【００３０】

本明細書で記載される他の処理フローと同様に、処理および処理の順序は変えられ得、変更され得および／または増大され得るが、それでもやはり望ましい成果を達成し得ることが理解される。例えば、トランスミッションのセンダについての固有の識別情報を抽出するステップへの随意的な追加は、トランスミッションのある部分（例えば、メッセージのヘッダにおける、送信したと称するドメインネーム（ｐｕｒｐｏｒｔｅｄ　ｓｅｎｄｉｎｇ　ｄｏｍａｉｎ　ｎａｍｅ））を、センダについての偽りでない（ｕｎｆｏｒｇｅａｂｌｅ）情報（例えば、トランスミッションの発信元であるＩＰアドレス）に認証するためのセンダ認証（ｓｅｎｄｅｒ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）手法を用いることであり得る。このプロセスは、フィルタリングシステムが、おそらく偽られており、認証されていない情報（例えば、ドメインネーム、または電子メールアドレス）に照会することにより、評判システム上のルックアップを行うことを可能にし得る。このようなドメイン、またはアドレスが肯定的な評判を有している場合には、トランスミッションは、全ての、またはいくつかのフィルタリング手法をバイパスすることによりレシピエントのシステムに直接送達され得る。このようなドメイン、またはアドレスが否定的な評判を有している場合には、フィルタリングシステムは、トランスミッションをドロップすることを選び得、それを隔離領域に保存することを選び得、または疑わしいとしてフラグを立てることを選び得る。

【００３１】

多くの異なるタイプのセンダ認証手法が使用され得る（例えば、センダポリシーフレームワーク（Ｓｅｎｄｅｒ　Ｐｏｌｉｃｙ　Ｆｒａｍｅｗｏｒｋ（ＳＰＦ））手法）。ＳＰＦはプロトコルであり、このプロトコルによって、ドメインの所有者は、どのＩＰアドレスが、既知のドメインに代わってメールを送信することを許可されているかを指示するＤＮＳレコードを公開する。他の限定されない例として、ＳｅｎｄｅｒＩＤ、またはＤｏｍａｉｎＫｅｙｓがセンダ認証手法として使用され得る。

【００３２】

別の例として、多くの異なるタイプの判定基準が、センダの通信の処理において使用され得る。図６は、評判スコアの決定における使用において、評判が良くない判定基準３００、および評判が良い判定基準３１０の使用を描いている。

【００３３】

評判が良くない判定基準３００、および評判が良い判定基準３１０は、評判が良くないセンダと、評判が良いセンダとを区別するために役立つ。判定基準のセットは、このスコアをつける手法を用いて生成された評判スコアに有意に影響することなく、しばしば変化し得る。ＳＰＡＭ識別のコンテキスト内の実例として、以下はメッセージのセンダの評判スコアをつけることに使用され得るスパム性判定基準のリストである。リストは網羅的であることを意図しておらず、観測された挙動に基づいて、他の判定基準を含むように、または判定基準を除去するように適合され得る。

１．平均スパムスコア（Ｍｅａｎ　Ｓｐａｍ　Ｓｃｏｒｅ）：センダが送信するトランスミッションの平均スパムプロファイラ（ｐｒｏｆｉｌｅｒ）スコアが、あるしきい値Ｗを超える場合には、センダは「評判が良くない」と宣言される。

２．ＲＤＮＳルックアップフェイラ（ＲＤＮＳ　Ｌｏｏｋｕｐ　Ｆａｉｌｕｒｅ）：リバース（ｒｅｖｅｒｓｅ）ドメインネームシステム（ＲＤＮＳ）が、センダのＩＰアドレスのフェイル（ｆａｉｌ）に照会する場合には、センダは「評判が良くない」と宣言される。

３．ＲＢＬメンバシップ（ＲＢＬ　Ｍｅｍｂｅｒｓｈｉｐ）：センダが、リアルタイムブラックホールリスト（ｒｅａｌ－ｔｉｍｅ　ｂｌａｃｋｈｏｌｅ　ｌｉｓｔ）（ＲＢＬ）に含まれる場合には、センダは「評判が良くない」と宣言される。（注意：複数のＲＢＬが使用され得る。ＲＢＬの各々は別個のテストの判定基準を構成し得る。）

４．メール量（Ｍａｉｌ　Ｖｏｌｕｍｅ）：センダの平均の（平均の、または中央値の）

トランスミッションの量がしきい値Ｘを超える場合には、センダは「評判が良くない」と宣言される。ここで、Ｘは期間におけるトランスミッションにおいて測定される（例えば、一日、一週間、または一ヶ月）。（注意：複数の期間における複数の平均量が使用され得、各々の平均量は別個のテストの判定基準を構成し得る。）

５．メールバースティネス／送信履歴（Ｍａｉｌ　Ｂｕｒｓｔｉｎｅｓｓ／Ｓｅｎｄｉｎｇ　Ｈｉｓｔｏｒｙ）：センダの平均の（平均の、または中央値の）トランスミッションのトラフィックパターンのバースティネス（ｂｕｒｓｔｉｎｅｓｓ）（より大きな期間（例えば、一日の活発な送信時間数、または一ヶ月の活発な送信日数）内の活発な送信サブピリオドの数により定義される）が、あるしきい値Ｙよりも小さい場合には、センダは「評判が良くない」と宣言される。ここでＹは、期間ごとのサブピリオドにおいて測定される。（注意：複数の期間において測定された複数の平均バースティネスが使用され得、各々の平均バースティネスの測定は別個のテストの判定基準を構成し得る。）

６．メールブレドス（Ｍａｉｌ　Ｂｒｅａｄｔｈ）：センダの平均の（平均の、または中央値の）トランスミッショントラフィックブレドス（ｂｒｅａｄｔｈ）（期間（例えば、一日、一週間、または一ヶ月）中に同一のセンダからのトランスミッションを受信するシステムのパーセンテージにより定義される）が、あるしきい値Ｚを超える場合には、センダは「評判が良くない」と宣言される。（注意：複数の期間における複数の平均ブレドスが使用され得、各々の平均ブレドス測定は、別個のテストの判定基準を構成し得る。）

７．マルウェアの活動（Ｍａｌｗａｒｅ　Ａｃｔｉｖｉｔｙ）：センダが、測定期間中に１つ以上のマルウェア（ｍａｌｗａｒｅ）コード（例えば、ウイルス、スパイウェア、侵入コード）を送達していることが知られている場合には、センダは「評判が良くない」と宣言される。

８．アドレスのタイプ（Ｔｙｐｅ　ｏｆ　Ａｄｄｒｅｓｓ）：インターネットサービスプロバイダ（ＩＳＰ）によって、ダイヤルアップの、またはブロードバンドの動的ホストコントロールプロトコル（ＤＨＣＰ）クライアントに動的に指定されたものとして知られている場合には、センダは「評判が良くない」と宣言される。

９．ＣＩＤＲブロックのスパム性（ＣＩＤＲ　Ｂｌｏｃｋ　Ｓｐａｍｍｉｎｅｓｓ）：センダのＩＰアドレスが、主に「評判が良くない」ＩＰアドレスを包含するクラスレスドメイン間ルーティング（ＣＩＤＲ）ブロック内に存在することが知られている場合には、センダは「評判が良くない」と宣言される。

１０．人的フィードバック（Ｈｕｍａｎ　Ｆｅｅｄｂａｃｋ）：センダが、コンテンツ、およびこれらのトランスミッションの他の特性を解析する人々により、所望されないトランスミッションが送信されることが報告される場合には、センダは「評判が良くない」と宣言される。

１１．スパムトラップフィードバック（ＳｐａｍＴｒａｐ　Ｆｅｅｄｂａｃｋ）：センダが、スパムトラップ（ｓｐａｍｔｒａｐ）として宣言され、任意の正当なトランスミッションを受信するように想定されていないものとして宣言されているアカウントにトランスミッションを送信する場合には、センダは「評判が良くない」と宣言される。

１２．バウンスバックフィードバック（Ｂｏｕｎｃｅｂａｃｋ　Ｆｅｅｄｂａｃｋ）：センダが、バウンスバック（ｂｏｕｎｃｅｂａｃｋ）トランスミッションを、またはトランスミッションを、送り先の（ｄｅｓｔｉｎａｔｉｏｎ）システムには存在しないアカウントに送信する場合には、センダは「評判が良くない」と宣言される。

１３．法律制定／標準の適合（Ｌｅｇｉｓｌａｔｉｏｎ／Ｓｔａｎｄａｒｄｓ　Ｃｏｎｆｏｒｍａｎｃｅ）：センダが、トランスミッションのセンダおよび／またはレシピエントのいずれかの動作する国において、トランスミッションの挙動の法律、規則、および確立された標準に従わない場合には、センダは「評判が良くない」と宣言される。

１４．動作の連続性（Ｃｏｎｔｉｎｕｉｔｙ　ｏｆ　Ｏｐｅｒａｔｉｏｎ）：センダが、あるしきい値Ｚよりも長く送信する位置において動作されない場合には、センダは「評判が良くない」と宣言される。

１５．レシピエントの需要に対する応答性（Ｒｅｓｐｏｎｓｉｖｅｎｅｓｓ　ｔｏ　Ｒｅ

ｃｉｐｉｅｎｔ　Ｄｅｍａｎｄｓ）：センダが、センダからの任意のこれ以上のトランスミッションを受信しないように、センダとの関係を終結させるためのレシピエントの正当な需要に対して合理的な時間枠において応答しない場合には、センダは「評判が良くない」と宣言される。

【００３４】

以下は、センダの「評判の良さ」の決定に使用され得る、「評判が良い」判定基準のリストである。リストは網羅的であることを意図しておらず、観測された挙動に基づいて、他の判定基準を含むように、または判定基準を除去するように適合され得る。

１．平均スパムスコア（Ｍｅａｎ　Ｓｐａｍ　Ｓｃｏｒｅ）：センダが送信するトランスミッションの平均スパムプロファイラスコアが、あるしきい値Ｗを下回る場合には、センダは「評判が良い」と宣言される。

２．人的フィードバック（Ｈｕｍａｎ　Ｆｅｅｄｂａｃｋ）：センダが、それらの送信ステーションが所属する組織の評判に関連する、そのセンダからのトランスミッションフローを解析する人々によって正当なトランスミッションのみを送信されることが報告されている場合には、センダは「評判が良い」と宣言される。

【００３５】

センダの世界において、各センダの評判の等級を計算した後に、評判の分類は、評判システムを利用する、照会するもの（ｑｕｅｒｉｅｒ）（例えばＤＮＳ、ＨＴＴＰなど）により解釈され得る通信プロトコルを経由して利用可能にされ得る。図７に示されているように、照会３５０がセンダに出されている場合には、評判システムは、センダのトランスミッションの受容性における最終的な判断を行うために、照会者により使用され得る任意の他の関連する付加的な情報だけでなく、センダの評判スコアをも含む戻り値（ｒｅｔｕｒｎ　ｖａｌｕｅ）３６０に応答し得る（例えば、判断スコアの年齢、スコアを決定する入力データなど）。

【００３６】

使用され得る通信プロトコルの例は、ドメインネームシステム（ＤＮＳ）サーバであり、ドメインネームシステムサーバは、ＩＰアドレス（１７２．ｘ．ｙ．ｚ）の形式の戻り値に応答し得る。ＩＰアドレスは、式：

【００３７】

【数８】

$$IP = 172.\left(\frac{rep - |rep|}{2 \times rep}\right).(|rep| div 256).(|rep| \bmod 256)$$

を用いてエンコードされ得る。

【００３８】

照会されたセンダの評判は、戻り値から以下のように：

ｒｅｐ＝（－１）^{z}×（２５６ｙ＋ｚ）

解読され得る。

【００３９】

それゆえ、ｘ＝０の場合に、戻ってきた評判は正の数で、ｘ＝１の場合に、戻ってきた評判は負の数である。評判の絶対値はｙおよびｚの値より決定される。このエンコードするスキームはサーバが、ＤＮＳプロトコルを経由して、評判の値を［－６５５３５，６５５３５］の範囲で戻すことを可能にする。それはまた、７（７）を、使用しないビットのままにする（すなわちｘの７つ高位のビットである）。これらのビットは、評判システムの拡張のために保存され得る。（例えば、評判スコアの年齢は、もとの照会するものへ通信され得る。）

図８は、４３０において、ネットワーク４４０上で受信されるトランスミッションを扱うためのシステムを描いている。トランスミッションは、多くの異なるタイプの通信であり得る（例えば、１つ以上のメッセージングエンティティ４５０から送信された電子メール（ｅ－ｍａｉｌ）メッセージ）。システム４３０は、メッセージングエンティティ４５

０からの通信を処理することを支援するためのフィルタリングシステム４６０を使用する。フィルタリングシステム４６０は、メッセージングエンティティ４５０からの通信に関連する特性を調査し、調査に基づいて、通信に関連する行動がとられる。例えば、通信は正当であると決定され得、従って、通信がフィルタリングシステム４６０によりフィルタされず、代わりに、意図されたレシピエントへの送達のための受信システム７０に提供される。

【００４０】

メッセージの適切な分類の精度を増加させるために（例えば、スパムまたは正当であるとして）、フィルタリングシステム４６０は、図９に示されるようなメッセージプロファイラプログラム５００によって構成され得る。メッセージプロファイラ５００は、図９に示されているようにメッセージを分類するための、複数のメッセージ分類手法、またはフィルタ５１０を使用する。メッセージプロファイラ５００が使用され得る、例示的なメッセージ分類手法、またはフィルタ５１０は：

・リバースＤＮＳ（Ｒｅｖｅｒｓｅ　ＤＮＳ（ＲＤＮＳ））－分類手法であって、（１）ドメインがセンダのＩＰアドレスのＤＮＳシステム内に存在するかどうかと、（２）このようなドメインが存在する場合には、ドメインが、センダがメッセージを送信することを要求するドメインと適合するかどうかの、チェックをするために、メッセージのセンダのＩＰアドレスに基づいて、リバースドメインネームサービス（ＤＮＳ）のルックアップを行う、分類手法。

・リアルタイムブラックホールリスト（Ｒｅａｌ－ｔｉｍｅ　Ｂｌａｃｋ－ｈｏｌｅ　Ｌｉｓｔ（ＲＢＬ））－分類手法であって、ＩＰアドレスが、任意のＲＢＬｓに不必要なメッセージを送信しそうなＩＰアドレスとして識別されないかどうかをチェックするために、メッセージのセンダのＩＰアドレスに基づいて、１つ以上のリアルタイムブラックホールリスト（ＲＢＬ）の照会を行う、分類手法。

・評判サーバ（Ｒｅｐｕｔａｔｉｏｎ　Ｓｅｒｖｅｒ）－分類手法であって、センダの評判を記述するスコアを受信するために、メッセージのセンダのＩＰアドレス、および／またはセンダのドメインネームおよび他のメッセージセンダの特性に基づいて、１つ以上の評判サーバの照会を行う、分類手法。

・サイン／指紋ベースの解析（Ｓｉｇｎａｔｕｒｅ／ｆｉｎｇｅｒｐｒｉｎｔｉｎｇ－ｂａｓｅｄ　Ａｎａｌｙｓｉｓ）（例えば、Ｓｔａｔｉｓｔｉｃａｌ　Ｌｏｏｋｕｐ　Ｓｅｒｖｉｃｅ（ＳＬＳ））－分類手法であって、メッセージのハッシュ（ｈａｓｈ）を計算し、算出されたメッセージのハッシュが、最近のメールフローにおいて、どのくらいの頻度で見られるかを決定するための、集中した統計的ルックアップサービス（ＳＬＳ）を照会する、分類手法。

・メッセージヘッダ解析による分類手法（Ｍｅｓｓａｇｅ　Ｈｅａｄｅｒ　Ａｎａｌｙｓｉｓ　Ｃｌａｓｓｉｆｉｃａｔｉｏｎ　Ｔｅｃｈｎｉｑｕｅ）－例として、この手法はＳｙｓｔｅｍ　Ｄｅｆｉｎｅｄ　Ｈｅａｄｅｒ解析（ＳＤＨＡ）、Ｕｓｅｒ　Ｄｅｆｉｎｅｄ　Ｈｅａｄｅｒ　Ａｎａｌｙｓｉｓ（ＵＤＨＡ）などを含み得る。

・システムに定義されるヘッダ解析（Ｓｙｓｔｅｍ　Ｄｅｆｉｎｅｄ　Ｈｅａｄｅｒ　Ａｎａｌｙｓｉｓ（ＳＤＨＡ））－分類手法のセットであって、メッセージを調査し、メッセージのヘッダが、おそらく不必要なメッセージのセンダを識別する傾向にある、特定のシステムに定義される特性を示すかどうかを識別する、セット。

・ユーザに定義されるヘッダ解析（Ｕｓｅｒ　Ｄｅｆｉｎｅｄ　Ｈｅａｄｅｒ　Ａｎａｌｙｓｉｓ（ＵＤＨＡ））－分類手法のセットであって、メッセージを調査し、メッセージのヘッダが、おそらく不必要なメッセージセンダを識別する傾向にある、あるシステムに定義される特性を示すかどうかを識別する、セット。

・センダ認証（Ｓｅｎｄｅｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）－分類手法のセットであって、（１）センダの要求されるドメインが、そのドメインにメールを送信するように権限を与えられたメールサーバの記録を公開しているかどうかと、（２）このような記録が公開されている場合には、記録が、要求されるドメインに代わってメールを送信するため

のセンダのＩＰアドレスに権限を与えるかどうかを決定するためにルックアップを行う、セット。一般的に使用されるＳｅｎｄｅｒ　Ａｕｔｈｅｎｔｉｃａｔｉｏｎ手法の例は、センダポリシーフレームワーク（ＳＰＦ）およびＳｅｎｄｅｒＩＤを含む。
・ベイジアンフィルタリング（Ｂａｙｅｓｉａｎ　Ｆｉｌｔｅｒｉｎｇ）－統計的な分類手法であって、メッセージにおけるテキストのトークン（ｔｏｋｅｎ）（単語）のセットに基づいて、メッセージが特定のカテゴリに分類される条件付き確率の結合の推定を算出する、手法。
・コンテンツフィルタリング（Ｃｏｎｔｅｎｔ　Ｆｉｌｔｅｒｉｎｇ）－分類手法であって、あるメッセージのカテゴリに関連している単語でメッセージのコンテンツを検索する、手法。
・クラスタリング分類（Ｃｌｕｓｔｅｒｉｎｇ　Ｃｌａｓｓｉｆｉｃａｔｉｏｎ）－特性の中の類似性の測定に基づく分類手法であって、通信は、望ましい、望ましくない（例えば、スパム）などとしてこのようなグループにクラスタされる。クラスタリングは、グループ内の類似性が高く、グループ間の類似性が低くなるように行われる。
リストは網羅的であることを意図されず、他の手法が発見された場合には他の手法を含むように適合され得る。リストの記載のいくつかは単一の手法を構成し、一方でその他のものは、多くの類似した、または密接に関連した手法の組み合わされたセットを構成する。複数の手法が共同で記述される場合には、メッセージプロファイラ５００は、各々の手法が、各々独自の信頼値を有することを認める。

【００４１】

メッセージプロファイラ５００は、しきい値ベースの手法を用いてメッセージを分類する。分類手法の各々５１０は、関連する信頼値５２０を有するメッセージプロファイラ５００により使用される。メッセージがプロファイリングに到達した場合には、メッセージプロファイラ５００は分類手法を介して繰り返し、各々の手法がメッセージを分類するように試みることを可能にする。各々の分類の結果は、［０，１］の範囲のデシマル値（ｄｅｃｉｍａｌ　ｖａｌｕｅ）である。各々の分類手法を介して繰り返した後に、メッセージプロファイラ５００は以下の式：

【００４２】

【数９】

$$Score = \sum_{i=1}^{N} SV_i \times C_i$$

を用いてメッセージにおけるスコアを算出する。ここで、SV_iは分類手法ｉに関連する信頼値、C_iは分類手法ｉにより生成された［０，１］における分類値である。

【００４３】

非線形のスコアリング関数による分類手法においては、以下の式が使用され得る：

【００４４】

【数１０】

$$Score = \sum_{i=1}^{N} (SV_{1i} \times C_i + SV_{2i} \times C_i^2)$$

ここで、SV_{1i}およびSV_{2i}は、分類手法ｉに関連する信頼値であり、C_iは、分類手法ｉにより生成された［０，１］における分類値である。

【００４５】

メッセージスコアが、５２０において決定された、ある特定のしきい値Ｔを超える場合には、次いでメッセージが第１の定義されたカテゴリに所属することを宣言される。メッセージスコアが、しきい値以下の場合には、反対のカテゴリに所属することを宣言される。システムは次いで、メッセージスコアにより到達したしきい値に基づく、適切な行動をとり得る（例えば、メッセージを隔離すること、メッセージをドロップすること（すなわち５３０において示されているように送達することなしにメッセージを消去すること）、

ある特定の文字列（ｓｔｒｉｎｇ）（例えば、「ＳＵＳＰＥＣＴＥＤ　ＳＰＡＭ」）を包含するようにメッセージの題（ｓｕｂｊｅｃｔ）を書き換えること、安全な送達のために、メッセージが暗号化エンジンを通ること、など）。システムはまた、複数のしきい値を特定すること、および各々のしきい値において異なる行動または異なる複数の行動を適用することを可能にし得、これらは分類の結果におけるメッセージプロファイラ５００の増加した信用を意味する。

【００４６】

メッセージプロファイラ５００の効果および精度は、いくつかの因子（例えば、分類手法５１０に関連するＳＶ$_i$、またはＳＶ$_{1i}$／ＳＶ$_{2i}$という信頼値５２０のセット）に依存している。調整可能なメッセージの分類構成は、値の最適なセットとともに、関連するしきい値および行動のセットを生成するために使用され得、それは、絶え間なく変化するメッセージフローパターン上で動作する分類手法のスコアの分布における頻繁に起こる変化に対して最新の保護を用いてアップデートされたメッセージプロファイラ５００を保持するために周期的に生成され得る。このように、メッセージプロファイラ構成は、ベクトル

（ＳＶ$_1$，ＳＶ$_2$，．．．，ＳＶ$_N$）

を含む（ベクトルは、全てのＮ個の分類手法の信頼値を表している）。図１０に示されているように、メッセージ分類チューナプログラム６００は、全ての起こりうるベクトルのベクトル空間を介して確率論的な検索を行うことにより、および予め選択されたしきい値において、プロファイラのフィルタリングの精度を最大にするベクトルを識別することによりメッセージプロファイラ５００を調整するように構成され得る。チューナ６００は、これを行うために異なるアプローチを用いる（例えば、発見的な（ｈｅｕｒｉｓｔｉｃ）アプローチ６１０を用いる）。

【００４７】

図１１は、ベクトル空間検索を行うための遺伝的アルゴリズム（ｇｅｎｅｔｉｃ　ａｌｇｏｒｉｔｈｍ）として知られる発見的アプローチを用いるチューナを図示している。遺伝的アルゴリズムを裏打ちするコンセプトは、進化論に由来し、そのアルゴリズムにおいて遺伝型（染色体を通じて表現される）は、その表現型（生物学的生物体として表現される）を通じて各々と競合する。時間につれて、生物学的進化は、生物体が進化するための環境において生存することが可能な、高く順応される、複雑な生物体を生成する。同様に、遺伝的アルゴリズムは、問題に対する候補解からなるベクトル空間を介して検索し、ここで、各々の候補解はベクトルとして表現される。多くのシミュレートされた候補解の世代において、遺伝的アルゴリズムは、問題に対してますます良く適合される解に向かって次第に進化する。

【００４８】

時間につれて、問題に対する良好な解を進化するための遺伝的アルゴリズムの能力は、他の候補解に比較して候補解の相対的なフィットネスレベルを評価するための正確なメカニズムの存在に依存する。従って、遺伝的アルゴリズム６５０は、実際の問題のドメインにおいて候補解のフィットネスを正確にモデル化する、フィットネス関数６６０を用いて設計される。

【００４９】

以下は、メッセージプロファイラ５００：

【００５０】

【数１１】

$$Fitness = \frac{\sum \left| S_{CAT1\_MISTAKES_i} - T \right|}{N_{CAT1}} + C \times \frac{\sum \left| S_{CAT2\_MIKSTAKES_j} - T + 1 \right|}{N_{CAT2}}$$

の最適化のために使用され得るフィットネス関数６６０である。関数における項の定義は以下のようになる：

Ｎ$_{CAT1}$＝第１のカテゴリに所属するデータセット全体からのメッセージベクトルの数

N_{CAT2}＝第２のカテゴリに所属するデータセット全体からのメッセージベクトルの数
Ｃ＝第２のカテゴリからの誤った分類をされたメッセージのための定数乗数
$S_{CAT1\_MISTAKEi}$＝他のカテゴリに所属するように誤った分類をされた第１のメッセージカテゴリからのメッセージベクトルｉのメッセージプロファイラスコア
$S_{CAT2\_MISTAKEi}$＝他のカテゴリに所属するように誤った分類をされた第２のメッセージカテゴリからのメッセージベクトルｉのメッセージプロファイラスコア
Ｔ＝メッセージプロファイラの数値しきい値で、しきい値を超えると、メッセージは第１のカテゴリに所属すると考慮される

関数は、構成が先に分類されたデータのセットにおけるメッセージベクトルを正確に分類しようとしてなされた、誤りに関連するコストを表現する。従って、低いフィットネス値は、遺伝的アルゴリズムの目的のために良く考慮される。関数における第１項は、第２のカテゴリに所属するように誤った分類をされた、第１のカテゴリからのメッセージに関連するコストを表現し（例えば、正当であると分類された望ましくないメッセージ、別名偽陰性（ｆａｌｓｅ　ｎｅｇａｔｉｖｅ））、第２項は、第１のカテゴリに所属するように誤った分類をされた、第２のカテゴリからのメッセージに関連するコストを表現する（例えば、望ましくないと分類された正当なメッセージ、別名偽陽性（ｆａｌｓｅ　ｐｏｓｉｔｉｖｅ））。総和は点の総数を表し、総和により、構成はメッセージベクトルを分類しようとする場合に誤りを生じた。直観的に、各々の項は、本質的に、分類エラーの平均の周波数と、分類エラーの平均の大きさ双方の表現である。第２項は定数Ｃを掛けられていることに注意されたい。この定数（２０という値にセットされ得る）は、一方のカテゴリからのメッセージの誤った分類の、反対のカテゴリからのメッセージの誤った分類に関連する、相対的なコストを表す。Ｃを２０にセットすることによって、これは、第２のカテゴリからのメッセージ上の分類の誤りが、第２のカテゴリからの誤りよりも２０倍費用のかかることを指示する。例えば、メッセージプロファイラ５００が、望ましい、および望ましくないメールの分類に使用される場合には、第１のカテゴリは望ましくないメール（例えば、スパム）を表し得、第２のカテゴリは正当なメッセージを表し得る。次いで、上記の関数は正当なメッセージの誤った分類（偽陽性）を、望ましくないメッセージの誤った分類（偽陰性）に比べ２０倍費用がかかると判断し得る。これは、偽陽性が偽陰性よりもかなり高いリスクを保有するような、反スパムコミュニティにおける現実世界の観点を反映する。メッセージプロファイラ５００が、ポリシーのコンプライアンスに関連する分類のために使用される場合には、偽陽性は、敏感な情報を含むが、メッセージプロファイラ５００によって、それ自体としてはラベルされず、結果として、組織がその特定のカテゴリに適用されるように選ばれ得るようなポリシーを回避させられるようなメッセージである。

【００５１】

図１２は、メッセージプロファイラが使用され得る動作シナリオを描いている。図１２を参照すると、動作シナリオは、ステップ７１０において、メッセージングエンティティからネットワーク上に送信された通信を受信することを含む。複数のメッセージ分類手法が、次いで７１０において、通信を分類するために使用される。メッセージ分類手法の各々は、信頼値に関連しており、信頼値は、メッセージ分類手法からのメッセージ分類出力の収集において使用される。各々の分類の出力は、数値、テキスト形式の値、またはカテゴリの値であり得る。メッセージ分類出力は、ステップ７３０においてメッセージプロファイラスコアを生成するためにステップ７２０において組み合わされる。メッセージプロファイラスコアは、メッセージングエンティティに関連する通信に対して、どんな行動がなされるべきかを決定するために、ステップ７４０において使用される。

【００５２】

本明細書で記載される他の処理フローと同様に、処理および処理の命令が、変えられ得、変更され得、および／または増大され得、まだ望ましい成果を達成し得ることが理解される。例えば、メッセージプロファイラは、メッセージを２つの区別できるカテゴリに適切に分類することが不可能な単一の手法が存在することを認識する動作シナリオにおいて

構成され得る（例えば、望ましい（正当な）および望ましくない（スパム、フィッシング（ｐｈｉｓｈｉｎｇ）、ウイルスなど）メッセージ通信間の区別、あるいは特有の組織のポリシー、法律、または規則をメッセージが遵守するかどうかの決定）。この動作シナリオにおいては、このような構成されたメッセージプロファイラは：
１．多くのメッセージ分類手法の結果を、アプリオリ（ａ　ｐｒｉｏｒｉ）にどの分類手法が使用されるかを特定することなく、分類の総計（例えば、「望ましくない」または「正当な」、「ＨＩＰＰＡ準拠」「ＧＬＢＡ違反」「ＨＲポリシー違反」など）に組み合わすためのフレームワークを提供するように設計され得、
２．手法の重要性のレベルが、時間につれる精度の変化を反映するように調整され得るように、分類手法の分類論理から、各分類手法の重要性（分類の総計への寄与として表現される）をデカップル（ｄｅｃｏｕｐｌｅ）するように設計され得、
３．フレームワークが、分類の総計において非常に正確な比率を達成するためにこの情報を使用するように調整され得るように、メカニズムを介して、フレームワーク内の分類手法の各々の相対的な重要性を記載し、それらの個別の精度の相関を記載するメカニズムを提供するように設計され得、
４．フレームワークが、ある環境において最大の分類精度に調整され得るように、メカニズムを介して、フレームワーク内の分類手法の各々の相対的な重要性を発見するためのメカニズムを提供するように設計され得る。
さらに、メッセージプロファイラは、他の動作シナリオにおいて動作するように構成され得る。例えば、図１３は、適応性のあるメッセージブロッキング、およびホワイトリスティング（ｗｈｉｔｅｌｉｓｔｉｎｇ）を用いて動作するように適合されているメッセージプロファイラを描いている。図１３を参照すると、個別のメッセージの分類に加え、メッセージプロファイラプログラム５００の総計された結果はまた、８２０において、それらのメッセージが受信しているメッセージプロファイラスコアの分配に基づいて、メッセージのセンダを分類するために用いられる。特有の時間枠（例えば、時間、日、週）の間に、特定のセンダ（例えばＩＰ）から受信されたメッセージの平均スコアが、特有のしきい値T_Uを超え、スコア分布がST_Uよりも小さな標準偏差を有する場合には、そのセンダは、「評判が悪い」に分類され得る（情報はデータ記憶装置８４０に記憶される）。プロセス８００は、このようなセンダに由来する全てのメッセージおよび接続が、次のＸ時間において処理することなく、８１０においてドロップされ得ることを決定するために、次いでデータ記憶装置８４０からのデータを使用する。これに対して、平均のスコアが、ST_Lよりも小さな標準偏差を有するしきい値T_L以下である場合には、センダは正当であると考えられ得（情報はデータ記憶装置８３０に記憶される）、そのセンダからのメッセージが、プロセス８００により、フィルタリング４６０において有意な処理のオーバヘッド、ネットワークのオーバヘッド、または記憶のオーバヘッドを引き起こす、特定のフィルタリング手法（例えば、メッセージプロファイラ５００のフィルタリング）をバイパスさせ得る。

【００５３】

メッセージプロファイラはまた、エンド（ｅｎｄｏ）、およびエクソ（ｅｘｏ）フィルタリングシステムの適応性のある訓練に関連して使用され得る。本明細書に記載されるセンダ分類のシステムおよび方法を用いることにより、メッセージプロファイラは、プロファイル内で使用される種々のフィルタリング手法の訓練のために、完全にプロファイルの外に位置するその他のものと同様に使用され得る。このような手法は、ベイジアン、サポートベクトルマシン（ＳＶＭ）、および他の統計学的な定常フィルタリング手法を、サインベースの手法（例えば、統計的なルックアップサービス（ＳＬＳ）およびメッセージクラスタリングタイプの手法）と同様に、含み得る。このような手法における訓練戦略は分類された、正当なおよび望ましくないメッセージのセットを使用し得、そのセットは、このようなセンダからのメッセージのスコアの総計から指定されたセンダの評判に基づいてメッセージプロファイラにより提供され得る。評判が悪いと分類されたセンダからのメッセージは、望ましくないとしてフィルタリングシステムのトレーナに提供され得、望まし

いメッセージが、正当なセンダにより送信されたストリームから取得される。

【００５４】

上記したように、メッセージプロファイラ５００は、１つの分類手法として、評判ベースのアプローチを使用し得る。図１４は、９００において、メッセージングエンティティ４５０からの、ネットワーク４４０上で受信されるトランスミッションを扱うことにおいて、フィルタリングシステム４６０によって使用され得る評判システムを描いている。より明確に、フィルタリングシステム４６０は、どんなフィルタリング行動が（ある場合には）メッセージングエンティティの通信上でとられるべきかの決定（少なくとも部分的に）を支援するために、評判システム９００を使用する。例えば、通信は評判が良い供給源からであると決定され得、結果として通信がフィルタされない。

【００５５】

フィルタリングシステム４６０は、９５０において受信された通信のセンダを識別し、その識別情報を評判システム９００に提供する。評判システム９００は、メッセージングエンティティが特定の特性を示す確率を計算することにより、照会されたセンダのアイデンティティの評判を評価する。全体の評判スコアは、計算された確率に基づいて決定され、フィルタリングシステム４６０に提供される。評判スコアは、値において、数値で、テキスト形式で、カテゴリ的であり得る。

【００５６】

フィルタリングシステム４６０は、９５２において、センダの通信においてどの行動がとられるべきかを決定する。フィルタリングシステム４６０は、評判システム９００からの評判スコアを、メッセージ分類フィルタとして使用し得、メッセージ分類フィルタは、その各々調整された信頼値を掛けられ、次いで他のメッセージ分類フィルタ結果と総計される。

【００５７】

評判システムは、フィルタリングシステムを補助するために多くの異なる方法で構成され得る。例えば、図１５は、評判スコアを計算するように構成されている評判システム９００を描いている。システムの構成１０００は、バイナリのテスト可能な判定基準１００２を識別することにより確立され得、テスト可能な判定基準１００２は、良いセンダと悪いセンダとの間の強いディスクリミネータであると思われる。Ｐ（ＮＲ｜Ｃ$_i$）は、それが質／判定基準Ｃ$_i$に従う場合には、センダは評判が良くないという確率として定義され得、Ｐ（Ｒ｜Ｃ$_i$）は、それが質／判定基準Ｃ$_i$に従う場合には、センダが評判である関数として定義され得る。

【００５８】

各々の質／判定基準Ｃ$_i$に対し、周期的な（例えば、一日の、一週間の、一ヶ月の、など）サンプリング演習は、Ｐ（ＮＲ｜Ｃ$_i$）を再計算するために行われ得る。サンプリング演習は、質／判定基準Ｃ$_i$が真であることが既知のセンダＮのランダムサンプルセットＳを選択することを含み得る。サンプル中のセンダは、次いで以下のセットの内の１つにソートされる：評判が良い（Ｒ）、評判が良くない（ＮＲ）、または未知（Ｕ）。Ｎ$_R$は、評判が良いセンダであるサンプルにおけるセンダ数であり、Ｎ$_{NR}$は、評判が良くないセンダのセンダ数、などである。次いで、Ｐ（ＮＲ｜Ｃ$_i$）およびＰ（Ｒ｜Ｃ$_i$）は、式：

【００５９】

【数１２】

$$P(NR \mid C_i) = \frac{N_{NR}}{N}$$

$$P(R \mid C_i) = \frac{N_R}{N}$$

を用いて推定される。この目的において、Ｎ＝３０は、各々の質／判定基準Ｃ$_i$において

Ｐ（ＮＲ｜Ｃ$_{i}$）およびＰ（Ｒ｜Ｃ$_{i}$）の正確な推定を達成するためには大きすぎるサンプルサイズであることが決定された。

【００６０】

全ての判定基準に対し、Ｐ（ＮＲ｜Ｃ$_{i}$）およびＰ（Ｒ｜Ｃ$_{i}$）を計算した後に、算出された確率は、評判スペースにおける各センダの、評判が良くない確率の総計Ｐ$_{NR}$　１００４、および評判が良いセンダの確率の総計Ｐ$_{R}$　１００６を計算するために使用される。これらの確率は式：

【００６１】

【数１３】

$$P_{NR}=\left(1-\prod_{i=1}^{N}\begin{cases}1-P(NR\mid C_i) & \text{判定基準}i\text{を適用した場合}\\ 1 & \text{それ以外の場合}\end{cases}\right)^{(\#\text{適用する判定基準の})}$$

$$P_{R}=\left(1-\prod_{i=1}^{N}\begin{cases}1-P(R\mid C_i) & \text{判定基準}i\text{を適用した場合}\\ 1 & \text{それ以外の場合}\end{cases}\right)^{(\#\text{適用する判定基準の})}$$

を用いて計算され得る。実験においては、上記の式は広範囲の入力判定基準の組み合わせの非常に良い挙動を見せ、実際には、それらの挙動は、入力判定基準の「評判が良くない」および「評判が良い」挙動の条件付き確率の単純な（ｎａｉｖｅ）結合を正確に算出するための式の挙動に類似するように見える。

【００６２】

各センダに対し、Ｐ$_{NR}$およびＰ$_{R}$を計算した後に、評判スコアは、そのセンダに対し以下の評判関数：

【００６３】

【数１４】

$$f(P_{NR},P_{R})=(c_1+c_2P_{NR}+c_2P_{R}+c_3P_{NR}^2+c_3P_{R}^2+c_4P_{NR}P_{R}+c_5P_{NR}^3+c_5P_{R}^3+c_6P_{NR}P_{R}^2+c_6P_{NR}^2P_{R})((P_{NR}-P_{R})^3+c_7(P_{NR}-P_{R}))$$

ここで

$$c_1=86.50$$
$$c_2=-193.45$$
$$c_3=-35.19$$
$$c_4=581.09$$
$$c_5=234.81$$
$$c_6=-233.18$$
$$c_7=0.51$$

を用いて計算される。異なる関数が、評判スコアのデタミネータ１００８として振舞い得、関数の表現に加えて、多くの異なる形式で表現され得ることが理解される。実例として、図１６は、１１００において評判スコアを決定するための表形式を描いている。表は、Ｐ$_{NR}$およびＰ$_{R}$の値に基づいて、それらが０．０～１．０の間で変動する場合に、上記の関数により生成される評判スコアを示している。例えば、１１１０に示されているように、５３という評判スコアはＰ$_{NR}$＝０．９およびＰ$_{R}$＝０．２の組み合わせにおいて取得される。この評判スコアは、センダが、評判が良いと考慮されない、比較的高い指標である。０という評判スコアは、Ｐ$_{NR}$およびＰ$_{R}$が同一である場合に取得される（例えば、１１２０において示されるように、Ｐ$_{NR}$＝０．７およびＰ$_{R}$＝０．７の場合には、評判スコアが０になる）。評判スコアは、Ｐ$_{R}$がＰ$_{NR}$よりも大きい場合に決定される、センダが比較的評判が良いことを指示するための負の値を有し得る。例えば、１１３０に示

されるように、P_{NR}＝０．５およびP_R＝０．８の場合には、評判スコアは－１２である。

【００６４】

多くの異なるタイプの判定基準が、評判システムのセンダの通信（例えば、評判スコアを決定するために、評判が良くない判定基準および評判が良い判定基準を用いること）の処理において使用され得る。このような判定基準の例は、２００４年１１月５日に出願され「ＣＬＡＳＳＩＦＩＣＡＴＩＯＮ　ＯＦ　ＭＥＳＳＡＧＩＮＧ　ＥＮＴＩＴＩＥＳ」と題名が付けられた、米国仮特許出願第６０／６２５，５０７号において開示されている。

【００６５】

本明細書で開示されるシステムおよび方法は、例としてのみ示されており、本発明の範囲を制限することを意味しない。上記したシステムおよび方法の他の変形は、当業者にとって明白であり、それ自体は本発明の範囲内であると考慮される。例えば、システムおよび方法は、多くの異なるタイプの通信を扱うように構成され得る（例えば、正当なメッセージ、あるいは望ましくない通信、または予め選択されたポリシーを侵害する通信である）。実例として、望ましくない通信は、スパムまたはウイルスの通信を含み得、予め選択されたポリシーは、企業の通信ポリシー、メッセージングポリシー、法律または規則のポリシー、あるいは国際通信ポリシーを含み得る。

【００６６】

本明細書で開示されたシステムおよび方法の、別の広範囲の例および変形として、システムおよび方法は種々のタイプのコンピュータアーキテクチャ上で（例えば、異なるタイプのネットワーク化された環境上で）インプリメントされ得る。実例として、図１７は、サーバアクセスアーキテクチャを描いており、サーバアクセスアーキテクチャにおいて、開示されたシステムおよび方法が使用され得る（例えば図１７の１３３０に示されているように）。この例におけるアーキテクチャは、企業のローカルネットワーク１２９０、およびローカルネットワーク１２９０内に備わっている種々のコンピュータシステムを備える。これらのシステムは、アプリケーションサーバ１２２０（例えば、ウェブサーバおよび電子メールサーバ）、ローカルクライアント１２３０を実行するユーザワークステーション（例えば、電子メールリーダおよびウェブブラウザ）、およびデータ記憶デバイス１２１０（例えばデータベースおよびネットワーク接続されたディスク）を備え得る。これらのシステムは、ローカル通信ネットワーク（例えばイーサネット（登録商標）（Ｅｔｈｅｒｎｅｔ（登録商標））１２５０）を通じてお互いに通信する。ファイアウォールシステム１２４０は、ローカル通信ネットワークとインターネット１２６０との間に備えられる。外部サーバのホスト１２７０および外部クライアント１２８０が、インターネット１２６０に接続されている。本開示は、構成要素間の通信を円滑にするために、インターネット、無線ネットワーク、ワイドエリアネットワーク、ローカルエリアネットワーク、およびこれらの組み合わせを含むがそれに制限されない、任意の種類のネットワークであり得ることが理解される。

【００６７】

ローカルクライアント１２３０は、ローカル通信ネットワークを通じて、アプリケーションサーバ１２２０、および共有のデータ記憶装置１２１０にアクセスし得る。外部クライアント１２８０は、インターネット１２６０を通じて外部アプリケーションサーバ１２７０にアクセスし得る。ローカルサーバ１２２０またはローカルクライアント１２３０が、外部サーバ１２７０へのアクセスを必要とする例、あるいは外部クライアント１２８０または外部サーバ１２７０が、ローカルサーバ１２２０へのアクセスを必要とする例においては、あるアプリケーションサーバに対し、適切なプロトコルにおける電子的な通信は、ファイアウォールシステム１２４０の「常にオープンな」ポートを介して流れる。

【００６８】

本明細書に記載したシステム１３３０は、イーサネット（登録商標）１２８０のようなローカル通信ネットワークに接続したハードウェアデバイス、または１つ以上のサーバ上に配置され得、ファイアウォールシステム１２４０と、ローカルサーバ１２２０およびロ

ーカルクライアント１２３０との間に、論理的に挿入され得る。ファイアウォールシステム１２４０を通って、ローカル通信ネットワークに入る、またはネットワークから出て行く、アプリケーションに関連する電子的な通信は、システム１３３０に経路付けられる。

【００６９】

図１７の例においては、システム１３３０は、非常に多くのセンダについての評判データを記憶し、処理するように、脅威マネジメントシステム（ｔｈｒｅａｔ　ｍａｎａｇｅｍｅｎｔ　ｓｙｓｔｅｍ）の一部として構成され得る。これは、脅威マネジメントシステムに、電子メール（ｅ－ｍａｉｌ）を許可するか、またはブロックするかについてのより良い説明を受けた上での決定（ｉｎｆｏｒｍｅｄ　ｄｅｃｉｓｉｏｎ）をさせ得る。

【００７０】

システム１３３０は、多くの異なるタイプの電子メールを扱うために使用され得、ＳＭＴＰおよびＰＯＰ３を含む、電子メールのトランスミッション、送達および処理のために使用される、多種のプロトコルを扱うために使用され得る。これらのプロトコルは、各々、サーバ間の電子メールメッセージを通信するための標準、および電子メールメッセージに関連するサーバクライアント通信のための標準を意味する。これらのプロトコルは、特にＩＥＴＦ（インターネット技術標準化委員会（Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｅｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ））によって普及されたＲＦＣ（リクエストフォーコメント（Ｒｅｑｕｅｓｔ　ｆｏｒ　Ｃｏｍｍｅｎｔｓ））において各々定義される。ＳＭＴＰプロトコルはＲＦＣ１２２１において定義され、ＰＯＰ３プロトコルはＲＦＣ１９３９において定義される。

【００７１】

これらの標準の開始以来、種々の必要性が電子メールの分野において進化し、エンハンスメントまたは付加的なプロトコルを含むさらなる標準の開発という結果を導いた。例えば、種々のエンハンスメントがＳＭＴＰ標準を進化させ、拡張ＳＭＴＰの進化という結果を導いた。拡張の例は、以下に見出され得る。（１）ＲＦＣ１８６９。上記ＲＦＣ１８６９は、手段（これによりサーバＳＭＴＰは、クライアントＳＭＴＰにそれがサポートするサービス拡張について通知し得る）を定義することにより、ＳＭＴＰサービスを拡張するためのフレームワークを定義する。（２）ＳＭＴＰサービスの拡張を定義するＲＦＣ１８９１。このことは、（ａ）送達ステータス通知（ｄｅｌｉｖｅｒｙ　ｓｔａｔｕｓ　ｎｏｔｉｆｉｃａｔｉｏｎ）が、ある状況下で生成されることと、（ｂ）このような通知がメッセージのコンテンツを戻すかどうかと、（ｃ）ＤＳＮが発行されるレシピエントと、オリジナルのメッセージが送達されたトランザクションの両方を、センダに識別させるＤＳＮと共に戻される付加的な情報と、をＳＭＴＰクライアントが明確にすることを可能にする。

【００７２】

加えて、ＩＭＡＰプロトコルは、ＰＯＰ３の代替物として進化し、電子メールサーバとクライアントとのさらに進んだ相互作用をサポートする。このプロトコルは、ＲＦＣ２０６０に記載される。

【００７３】

他の通信メカニズムもまた、ネットワーク上で広く使用される。これらの通信メカニズムは、ボイスオーバーＩＰ（ＶｏＩＰ（Ｖｏｉｃｅ　Ｏｖｅｒ　ＩＰ））およびインスタントメッセージを含むが、制限されない。ＶｏＩＰはＩＰ電話において、インターネットプロトコル（ＩＰ）を用いる音声情報の送達を扱うための機能のセットを提供するために使用される。インスタントメッセージは、リアルタイムに通信（例えば、会話）を送達するインスタントメッセージサービスに接続するクライアントを含む通信タイプである。

【００７４】

インターネットがより広く使用されるにつれて、インターネットはまた、ユーザにとって新たなトラブルを作り出した。特に、個別のユーザにより受信されるスパムの量は、ここしばらくの間で劇的に増加している。本明細書で使用されるスパムは、レシピエントにより依頼されていない、または望まれていない任意の通信を受け取ることをいう。システ

ムおよび方法は、本明細書において開示されるように、これらのタイプの依頼されていない、または望まれていない通信をアドレスするように構成され得る。これは、電子メールをスパムすることが、企業の資源を消費することおよび生産性に影響を与えることにおいて有用であり得る。

【００７５】

本明細書で公開されるシステムおよび方法は、１つ以上のデータ処理デバイスとの通信のために、ネットワーク（例えば、ローカルエリアネットワーク、ワイドエリアネットワーク、インターネットなど）、光ファイバ媒体、搬送波、無線ネットワークなどを通じて伝達されたデータ信号を用い得る。データ信号は、本明細書で公開される、デバイスへ提供される、またはデバイスから提供される、任意の、または全てのデータを運び得る。

【００７６】

さらに、本明細書に記載される方法およびシステムは、１つ以上のプロセッサにより実行可能なプログラム命令を含むプログラムコードにより、多くの異なるタイプの処理デバイス上でインプリメントされ得る。ソフトウェアプログラム命令は、処理システムに、本明細書で記載される方法を行わせるように動作可能なソースコード、オブジェクトコード、マシンコードまたは任意の他の記憶されたデータを含み得る。

【００７７】

システムの、および方法のデータ（例えば、アソシエーション、マッピングなど）は、異なるタイプの記憶デバイスおよびプログラミング構造物（例えば、データ記憶装置、ＲＡＭ、ＲＯＭ、フラッシュメモリ、単層ファイル、データベース、プログラミングデータ構造、プログラミング変数、ＩＦ－ＴＨＥＮ（または類似のタイプの）命令文構造物など）のような１つ以上の異なるタイプのコンピュータインプリメントの方法において記憶およびインプリメントされ得る。データ構造は、コンピュータプログラムによる使用のためのデータベース、プログラム、メモリまたは他のコンピュータ読み取り可能な媒体において、データを編成することおよび記憶することに使用するためのフォーマットを記述することに注意されたい。

【００７８】

システムおよび方法は、方法の動作を行うために、および本明細書に記載されるシステムをインプリメントするために、プロセッサによる実行において使用される命令を包含するコンピュータの記憶メカニズム（例えば、ＣＤ－ＲＯＭ、ディスケット、ＲＡＭ、フラッシュメモリ、コンピュータのハードドライブなど）を含む、多くの異なるタイプのコンピュータ読み取り可能な媒体に提供され得る。

【００７９】

本明細書に記載される、コンピュータのコンポーネント、ソフトウェアモジュール、機能およびデータ構造は、それらの動作に必要とされるデータのフローを許容するために、お互いに、直接的にまたは間接的に接続し得る。ソフトウェア命令またはモジュールは、例えば、コードのサブルーチンユニットとして、コードのソフトウェア機能ユニットとして、オブジェクト（オブジェクト指向のパラダイムなどの場合）として、アプレットとして、コンピュータスクリプト言語において、別のタイプのコンピュータコードまたはファームウェアとして、インプリメントされ得ることにも注意されたい。ソフトウェアのコンポーネントおよび／または機能性は、単一のデバイス上に配置され得、当面の状況に依存して複数のデバイスにわたり分配され得る。

【００８０】

本明細書の記載および添付する請求の範囲全体にわたって使用される場合には、「１つの（ａ）」「１つの（ａｎ）」および「該」の意味は、文脈上他に明確に指図する場合を除いて、複数の参照を含むことが理解される。また、本明細書の記載および添付する請求の範囲全体にわたって使用される場合には、「において」の意味は、文脈上他に明確に指図する場合を除いて、「の中で」および「上で」を含む。最後に、本明細書の記載および添付する請求の範囲全体にわたって使用される場合には、「および」および「または」の意味は、文脈上他に明確に指図する場合を除いて、接続詞および離接接続詞の双方を含み

、交換できるように使用され得る。フレーズ「排他的なまたは」は離説接続詞の意味のみが適用され得る状況を指示するために使用され得る。

【図面の簡単な説明】

【００８１】

【図１】図１は、ネットワーク上で受信されたトランスミッションを扱うシステムを描いているブロック図である。

【図２】図２は、評判スコアを決定するように構成されている評判システムを描いているブロック図である。

【図３】図３は、種々の計算された確率の値における評判スコアを描いている表である。

【図４】図４は、種々の計算された確率の値における評判スコアを描いているグラフである。

【図５】図５は、評判スコアを生成するための動作シナリオを描いているフローチャートである。

【図６】図６は、評判スコアを決定するための、評判が良くない判定基準および評判が良い基準の使用を描いているブロック図である。

【図７】図７は、センダの評判スコアを含む戻り値に応答するように構成された評判システムを描いているブロック図である。

【図８】図８は、ネットワーク上で受信されるトランスミッションを扱うためのシステムを描いているブロック図である。

【図９】図９は、メッセージプロファイラプログラムを有するフィルタリングシステムを描いているブロック図である。

【図１０】図１０は、メッセージ分類チューナプログラムを描いているブロック図である。

【図１１】図１１は、メッセージ分類チューナプログラムとしての遺伝的アルゴリズムの使用を描いているブロック図である。

【図１２】図１２は、メッセージプロファイラが使用される動作シナリオを描いているフローチャートである。

【図１３】図１３は、適応性のあるメッセージブロッキングおよびホワイトリスティングによって動作するように適合されているメッセージプロファイラを描いているブロック図である。

【図１４】図１４は、ネットワーク上で受信されたトランスミッションを扱うための評判システムを描いているブロック図である。

【図１５】図１５は、評判スコアを決定するために構成されている評判システムを描いているブロック図である。

【図１６】図１６は、種々の計算された確率の値における評判スコアを描いている表である。

【図１７】図１７は、サーバアクセスアーキテクチャを描いているブロック図である。

【図１】

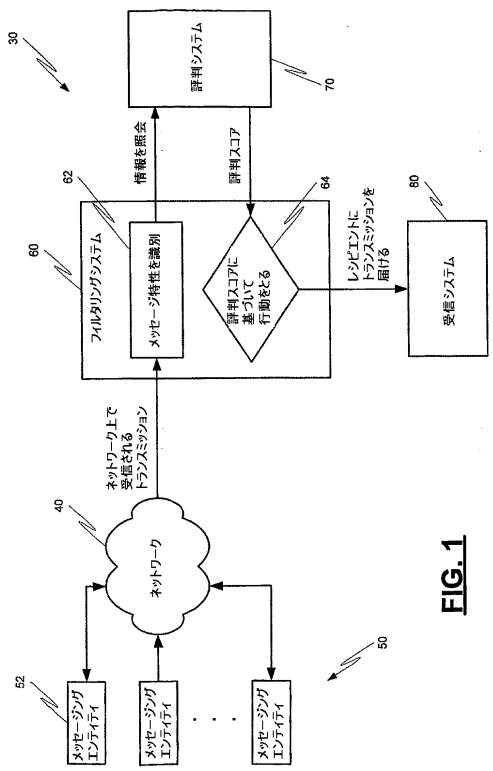

FIG. 1

【図２】

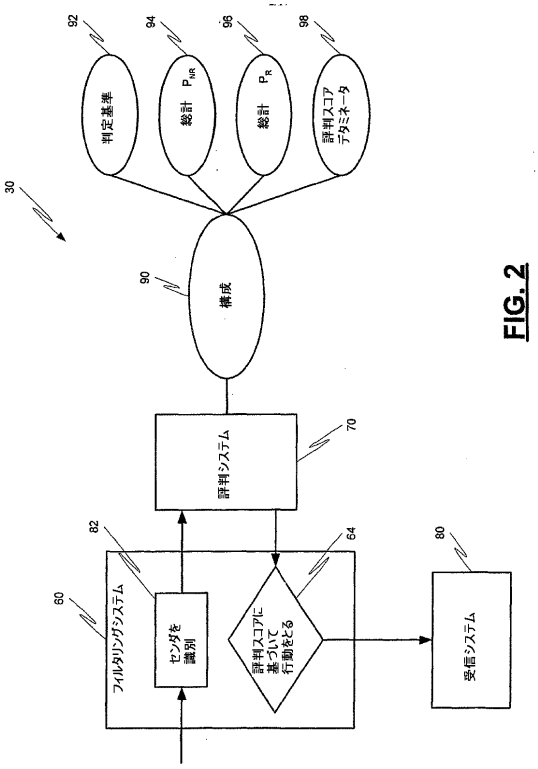

FIG. 2

【図３】

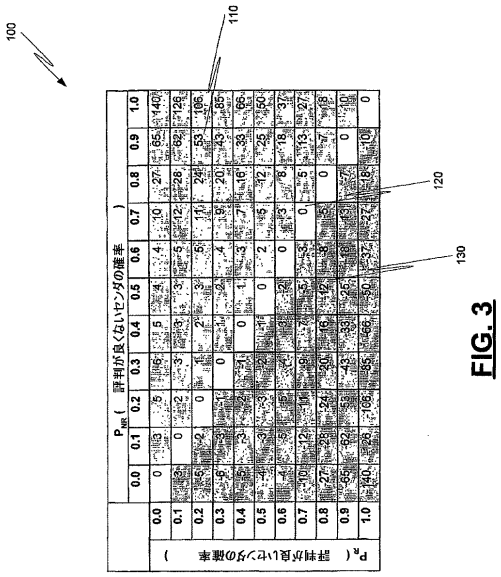

FIG. 3

【図４】

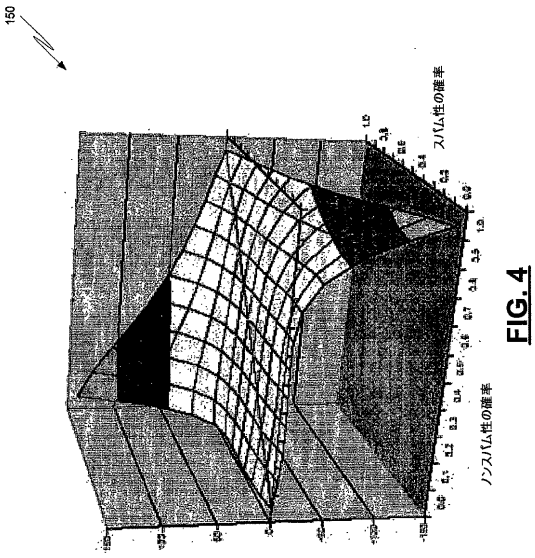

FIG. 4

【図５】

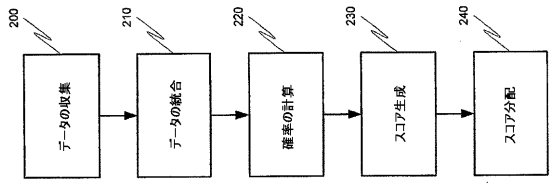

FIG. 5

【図６】

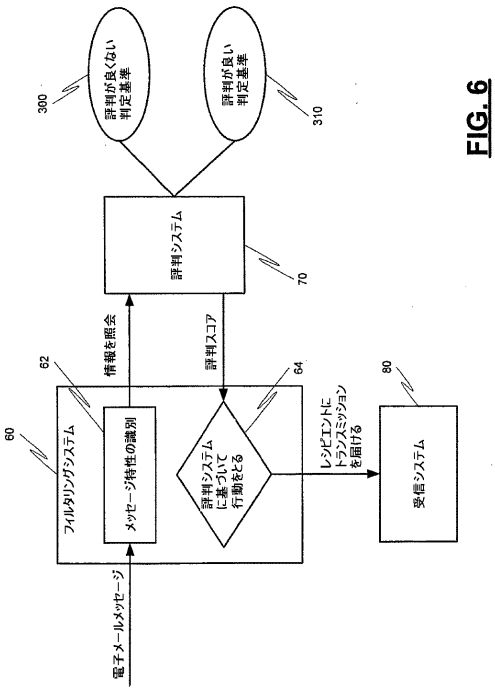

FIG. 6

【図７】

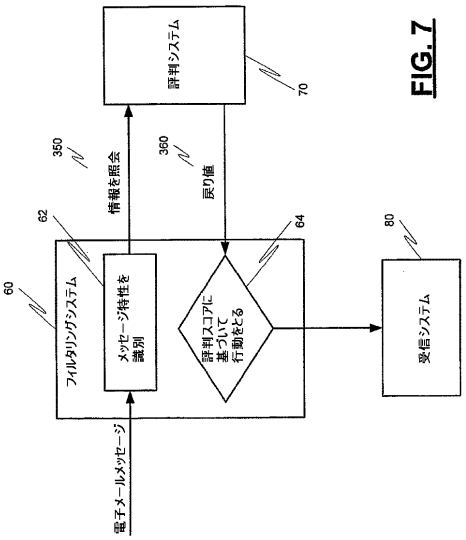

FIG. 7

【図８】

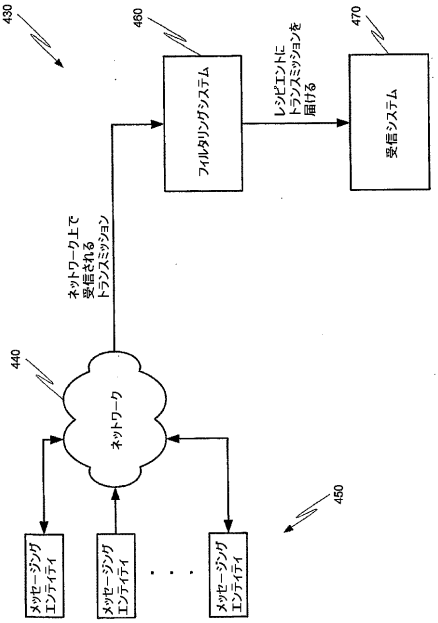

FIG. 8

【図９】

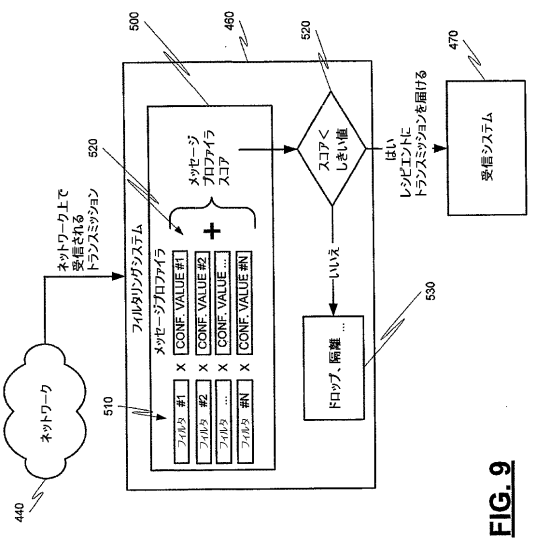

FIG. 9

【図１０】

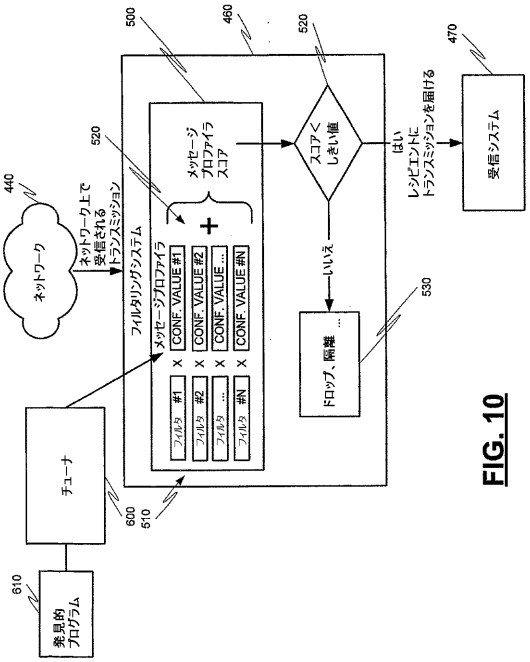

FIG. 10

【図１１】

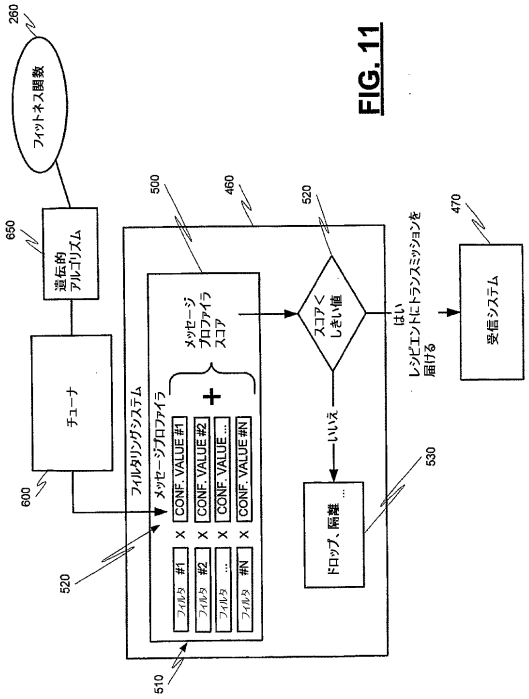

FIG. 11

【図１２】

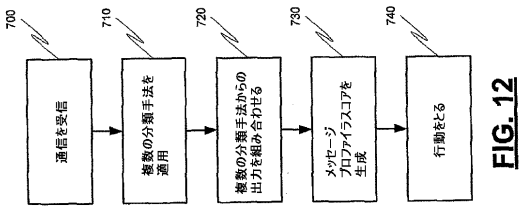

FIG. 12

【図１３】

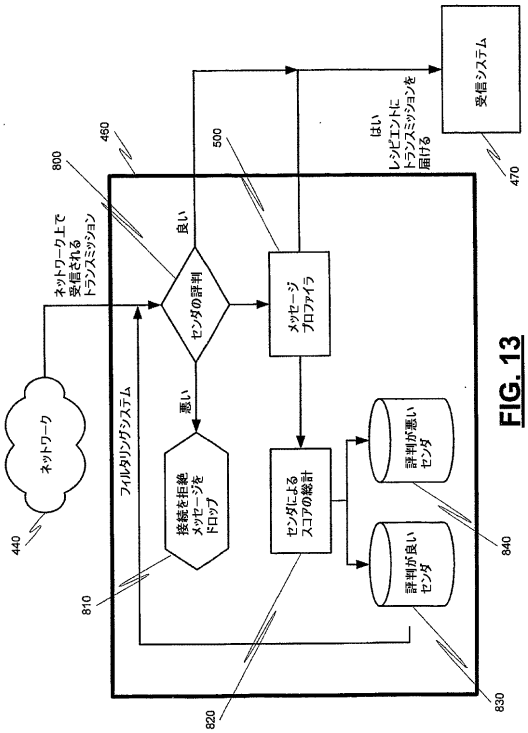

FIG. 13

【図１４】

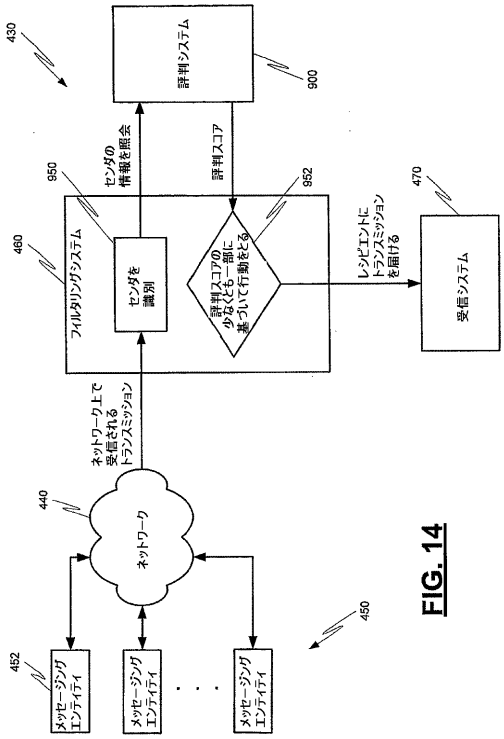

FIG. 14

【図１５】

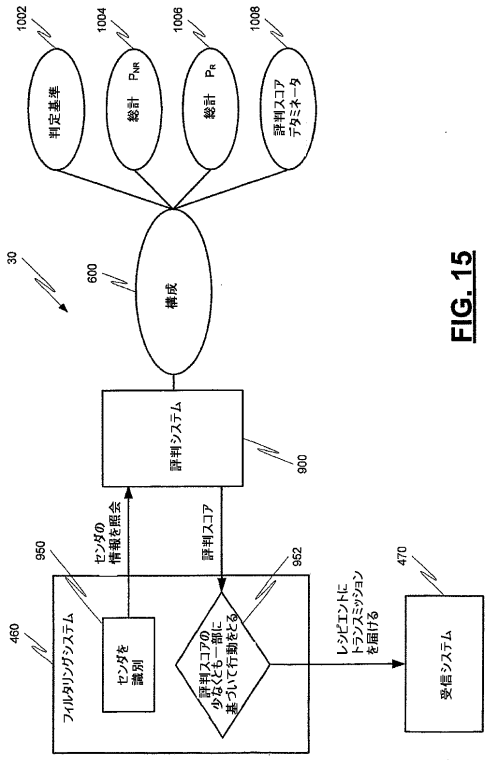

FIG. 15

【図１６】

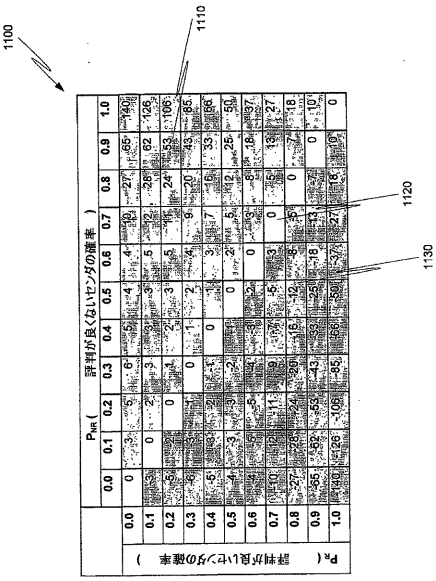

FIG. 16

【図１７】

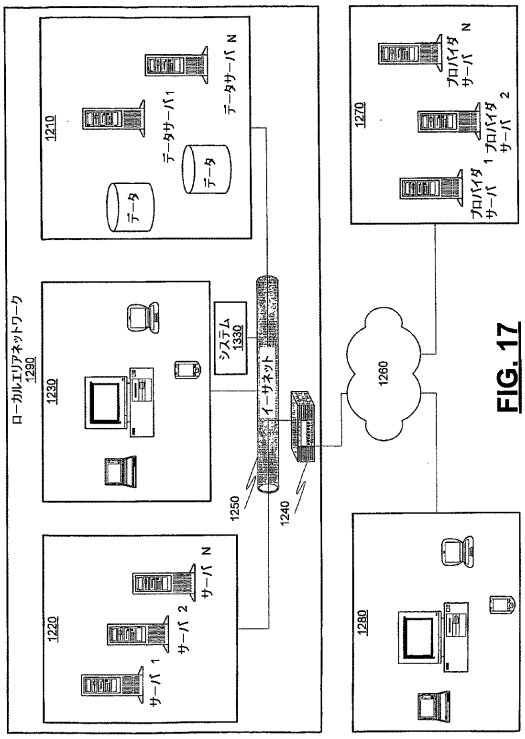
ローカルエリアネットワーク
1290
1210
データサーバ1
データサーバN
データ
データ
1230
システム
1330
イーサネット
1250
1240
1220
サーバ1
サーバ2
サーバN
1260
1270
プロバイダサーバ1
プロバイダサーバ2
プロバイダサーバN
1280

FIG. 17

フロントページの続き

(31)優先権主張番号 11/173,941
(32)優先日 平成17年7月1日(2005.7.1)
(33)優先権主張国 米国(US)

(72)発明者 ジャッジ, ポール
アメリカ合衆国 ジョージア ３００２２, アルファレッタ, ジョーンズ ブリッジ ロード １００９０, ユニット ３
(72)発明者 ラジャン, グル
アメリカ合衆国 ジョージア ３００９７, ダルース, スタンフォード リッジ １６５
(72)発明者 アルペロヴィッチ, ドミトリ
アメリカ合衆国 ジョージア ３０３２６, アトランタ, ピーチツリー ロード エヌイー ３３３８ ナンバー１００３
(72)発明者 モイヤー, マット
アメリカ合衆国 ジョージア ３００４４, ローレンスビル, アラモサ コート ３７２１

審査官 玉木 宏治

(56)参考文献 国際公開第２００４／０８８４５５（WO，Ａ１）
米国特許出願公開第２００４／０１７７１２０（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 12/00-66
G06F 13/00