(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5352764号
(P5352764)
(45)発行日　平成25年11月27日(2013.11.27)　(24)登録日　平成25年9月6日(2013.9.6)

(51)Int.Cl.　F I
H04L 12/58 (2006.01)　H04L 12/58 100Z

請求項の数 34 (全 21 頁)

(21)出願番号　特願2009-549019(P2009-549019)
(86)(22)出願日　平成19年11月9日(2007.11.9)
(65)公表番号　特表2010-518737(P2010-518737A)
(43)公表日　平成22年5月27日(2010.5.27)
(86)国際出願番号　PCT/NL2007/050557
(87)国際公開番号　WO2008/097077
(87)国際公開日　平成20年8月14日(2008.8.14)
審査請求日　平成22年11月8日(2010.11.8)
(31)優先権主張番号　1033356
(32)優先日　平成19年2月8日(2007.2.8)
(33)優先権主張国　オランダ(NL)

前置審査

(73)特許権者　513149540
スシッピオ・ホールディング・ベー・フェー
オランダ・４８７４・エルフェー・エテン－ルール・ラークセヴェク・２４
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】電子メッセージの拡散を減少させる方法およびシステム

(57)【特許請求の範囲】
【請求項１】
電子メッセージを少なくとも第１ユーザ機器（Ｉ）および第２ユーザ機器（ＩＩ）に送信するように構成された１つまたは複数のサーバを備えるサーバシステム（１）において電子メッセージの拡散を減少させる方法であって、
前記サーバシステムが、
前記サーバシステムにおいて電子メッセージまたはその一部を受信するステップ（３０；５０）と、
前記電子メッセージまたはその一部を前記第１ユーザ機器（Ｉ）に提供するステップ（３１；５１）と、
前記電子メッセージまたはその一部に関する少なくとも１つのスパム通知信号を前記第１ユーザ機器（Ｉ）から受信するステップと、
前記第１ユーザ機器（Ｉ）からの前記少なくとも１つのスパム通知信号の受信に応答してのみ、前記サーバシステム（１）からの前記電子メッセージの前記第２ユーザ機器（ＩＩ）へのダウンロードを阻止し、または、表示を阻止するステップ（３３；５５）と、
を有し、
前記少なくとも１つのスパム通知信号のうちのスパム通知信号は、前記サーバシステムからの前記電子メッセージのダウンロードを阻止し、または、表示を阻止する、前記サーバシステムへの指示である方法。
【請求項２】

前記サーバシステム（１）が第３ユーザ機器（ＩＩＩ）から前記電子メッセージを受信するステップをさらに有し、前記第１、第２、および、第３ユーザ機器のユーザは集約的に登録される請求項１に記載の方法。

【請求項３】

前記ユーザの各々には、前記サーバシステム（１）にアクセスするためのユーザアドレスおよびユーザ固有のパスワードを含むユニークなログインコードが与えられる請求項２に記載の方法。

【請求項４】

前記サーバシステム（１）が、安全な方法で前記電子メッセージおよび前記スパム通知信号を送信および受信するステップをさらに有する請求項１から３のいずれか一項に記載の方法。

【請求項５】

前記サーバシステム（１）は少なくとも第１サーバ（１Ｃ）および第２サーバ（１Ａ，１Ｂ）を備え、

前記第１サーバ（１Ｃ）において前記電子メッセージを受信するステップ（５０）と、

前記第１サーバ（１Ｃ）において前記電子メッセージを記憶するステップと、

前記電子メッセージの一部を前記第２サーバ（１Ａ，１Ｂ）に送信するステップ（５１）と、

前記第２サーバにおいて前記電子メッセージの一部を受信するステップと、

前記第２サーバ（１Ａ，１Ｂ）から前記第１ユーザ機器（Ｉ，ＩＩ）に前記電子メッセージの一部を提供するステップ（５２）と、

前記電子メッセージの一部の選択に応答して、前記第１サーバ（１Ｃ）から前記第１ユーザ機器（Ｉ，ＩＩ）に前記電子メッセージを提供するステップ（５３）と、

をさらに有する請求項１から４のいずれか一項に記載の方法。

【請求項６】

前記第１サーバ（１Ｃ）において前記スパム通知信号を受信するステップをさらに有する請求項５に記載の方法。

【請求項７】

前記電子メッセージの複数の複製を提供するステップをさらに有し、前記電子メッセージの複製の数は前記電子メッセージの受取人の数より小さい請求項５または６に記載の方法。

【請求項８】

前記第１サーバ（１Ｃ）において１回のみ前記電子メッセージを記憶するステップをさらに有する請求項５または６に記載の方法。

【請求項９】

前記スパム通知信号に応答して、前記第１サーバ（１Ｃ）において前記電子メッセージを削除し、かつ／または、前記第２サーバ（１Ａ，１Ｂ）において前記電子メッセージの一部を削除するステップをさらに有する請求項６に記載の方法。

【請求項１０】

前記サーバシステム（１）が、

前記電子メッセージについて前記第１ユーザ機器（Ｉ）から前記スパム通知信号を受信するステップと、

前記スパム通知信号が受信された電子メッセージの送信者の送信者識別情報を記憶するステップと、

前記送信者から１つまたは複数の他の電子メッセージを受信するステップと、

前記送信者識別情報を使用して前記第１ユーザ機器（Ｉ）および前記第２ユーザ機器（ＩＩ）のうち少なくとも１つについて前記他の電子メッセージのうち少なくとも１つへのアクセスを制限するステップと、

をさらに有する請求項１から９のいずれか一項に記載の方法。

【請求項１１】

前記他の電子メッセージへのアクセスを制限するステップは、
特定の期間について前記他の電子メッセージへのアクセスを制限するステップ、
前記他の電子メッセージの一部へのアクセスを制限するステップ、
前記送信者と１または複数の受取人との間の通信履歴に依存して前記他の電子メッセージの受取人について前記他の電子メッセージへのアクセスを制限するステップ、
のうち少なくとも１つを含む請求項１０に記載の方法。
【請求項１２】
前記期間または前記一部は、
前記送信者の電子メッセージについて受信されたスパム通知信号の数、
前記送信者の電子メッセージについてアクセスが制限された回数、
のうち少なくとも１つによって決定される請求項１１に記載の方法。
【請求項１３】
前記スパム通知信号が受信された電子メッセージの送信者に警告メッセージを送信するステップをさらに有する請求項１から１２のいずれか一項に記載の方法。
【請求項１４】
前記スパム通知信号が受信された電子メッセージの送信者について前記サーバシステム（１）へのアクセスを制限するステップをさらに有する請求項１から１３のいずれか一項に記載の方法。
【請求項１５】
前記アクセスを制限するステップは、
特定の送信者の電子メッセージについて受信されたスパム通知信号の数、
前記送信者の電子メッセージについてアクセスが制限された回数、
前記送信者と、前記電子メッセージの１または複数の受取人との間の通信履歴、
のうち少なくとも１つに依存する請求項１４に記載の方法。
【請求項１６】
前記方法のステップはスパムフィルタの動作とは関係なく実行され、前記スパムフィルタは前記サーバシステムによって受信された電子スパムメッセージを検出するためにスパムルールの集合を用いる請求項１から１５のいずれか一項に記載の方法。
【請求項１７】
電子システムにインストールされ、電子システムによって実行されるとき、請求項１から１６のいずれか一項に記載の方法を実行するように構成されたソフトウェアコード部分を有するコンピュータプログラム。
【請求項１８】
請求項１７に記載のコンピュータプログラムを含む担体。
【請求項１９】
電子メッセージを少なくとも第１ユーザ機器（Ｉ）および第２ユーザ機器（ＩＩ）に送信するように構成された１つまたは複数のサーバを備えるサーバシステム（１）であって、前記サーバシステムは、前記電子メッセージの拡散を減少させるように構成され、
電子メッセージまたはその一部を受信するように構成された電子メッセージ受信部（１３）と、
前記電子メッセージまたはその一部を前記第１ユーザ機器（Ｉ）に提供するように構成された電子メッセージ提供部（１４）と、
前記電子メッセージまたはその一部に関する少なくとも１つのスパム通知信号を前記第１ユーザ機器（Ｉ）から受信するように構成されたスパム通知受信部（１５）と、
前記第１ユーザ機器（Ｉ）からの前記少なくとも１つのスパム通知信号の受信に応答してのみ、前記サーバシステム（１）からの前記電子メッセージの前記第２ユーザ機器（ＩＩ）へのダウンロードを阻止し、または、表示を阻止するように構成されたアクセス制限部（１６）と、
を備え、
前記少なくとも１つのスパム通知信号のうちのスパム通知信号は、前記サーバシステム

からの前記電子メッセージのダウンロードを阻止し、または、表示を阻止する、前記サーバシステムへの指示であるサーバシステム（１）。

【請求項２０】

前記サーバシステムは、前記サーバシステムにアクセスするために必要なユーザアドレスおよびユーザ固有のパスワードを含むユニークなログインコードを記憶するレジスタ（１７）を備える請求項１９に記載のサーバシステム（１）。

【請求項２１】

前記サーバシステムは、さらに、第３ユーザ機器（ＩＩＩ）から電子メッセージを受信するように構成され、前記サーバシステムは、前記第１、第２、および、第３ユーザ機器との通信を安全にするための手段（１８）を備える請求項１９または２０に記載のサーバシステム（１）。

【請求項２２】

前記サーバシステムは少なくとも第１サーバ（１Ｃ）および第２サーバ（１Ａ，１Ｂ）を備え、

前記第１サーバ（１Ｃ）は、

前記電子メッセージを受信する電子メッセージ受信部と、

前記電子メッセージを記憶する記憶手段と、

前記受信された電子メッセージに基づいて前記電子メッセージの一部を提供するように構成された部分提供部と、

前記電子メッセージの一部を前記第２サーバに送信する送信部と、

前記第１ユーザ機器からの前記電子メッセージの要求の受信に応答して、前記電子メッセージを前記第１ユーザ機器に送信する送信部と、

を備え、

前記第２サーバ（１Ａ，１Ｂ）は、

前記第１サーバの送信部から前記電子メッセージの一部を受信するように構成された電子メッセージ部分受信部と、

前記第１ユーザ機器に前記電子メッセージの一部を提供する手段と、

を備える請求項１９から２１のいずれか一項に記載のサーバシステム（１）。

【請求項２３】

前記第１サーバ（１Ｃ）は、前記第１ユーザ機器からスパム通知信号を受信するように構成されたスパム通知信号受信部をさらに備える請求項２２に記載のサーバシステム（１）。

【請求項２４】

前記サーバシステムは、前記電子メッセージの複数の複製を提供するように構成され、前記電子メッセージの複製の数は前記電子メッセージの受取人の数より小さい請求項１９から２３のいずれか一項に記載のサーバシステム（１）。

【請求項２５】

前記第１サーバの記憶手段のみが前記電子メッセージを記憶するように構成された請求項２２から２４のいずれか一項に記載のサーバシステム（１）。

【請求項２６】

前記スパム通知信号に応答して、前記第１サーバにおいて前記電子メッセージを削除し、前記第２サーバにおいて前記電子メッセージの一部を削除することを指示するように構成された電子メッセージ削除部および電子メッセージ部分削除部を備える請求項２２から２５のいずれか一項に記載のサーバシステム（１）。

【請求項２７】

前記サーバシステムは、前記スパム通知信号受信部がスパム通知信号を受信した電子メッセージの送信者の送信者識別情報を記憶するように構成された送信者識別情報記憶部をさらに備え、

前記電子メッセージ受信部（１３）は、他の電子メッセージを受信するように構成され、

前記アクセス制限部は、前記送信者識別情報を使用して前記第１ユーザ機器（Ｉ）および前記第２ユーザ機器（ＩＩ）のうち少なくとも１つについて前記他の電子メッセージのうち少なくとも１つへのアクセスを制限するように構成された請求項１９から２６のいずれか一項に記載のサーバシステム（１）。

【請求項２８】

前記アクセス制限部（１６）は、さらに、

特定の期間について前記他の電子メッセージへのアクセスを制限するステップ、

前記他の電子メッセージの一部へのアクセスを制限するステップ、

前記送信者と１または複数の受取人との間の通信履歴に依存して前記他の電子メッセージの受取人について前記他の電子メッセージへのアクセスを制限するステップ、

のうち少なくとも１つを実行するように構成された請求項２７に記載のサーバシステム（１）。

【請求項２９】

前記送信者の電子メッセージについて受信されたスパム通知信号の数をカウントするように構成されたカウンタ（２１）、

前記送信者の電子メッセージについてアクセスが制限された回数をカウントするように構成されたカウンタ（２１）、

のうち少なくとも１つをさらに備える請求項２８に記載のサーバシステム（１）。

【請求項３０】

前記スパム通知信号が受信された電子メッセージの送信者に警告メッセージを送信するように構成された警告メッセージ送信部（２２）をさらに備える請求項１９から２９のいずれか一項に記載のサーバシステム（１）。

【請求項３１】

前記スパム通知信号が受信された電子メッセージの送信者について前記サーバシステムへのアクセスを制限するように構成されたアクセス制限部（２３）をさらに備える請求項１９から３０のいずれか一項に記載のサーバシステム（１）。

【請求項３２】

特定の送信者の電子メッセージについて受信されたスパム通知信号の数、

前記送信者の電子メッセージについてアクセスが制限された回数、

前記送信者と、前記電子メッセージの１または複数の受取人との間の通信履歴、

のうち少なくとも１つに依存して前記サーバシステムへのアクセスを制限するように構成された評価モジュール（２４）をさらに備える請求項３１に記載のサーバシステム（１）。

【請求項３３】

前記サーバシステムはスパムフィルタとは関係なく動作するように構成され、前記スパムフィルタは電子スパムメッセージを検出するためにスパムルールの集合を用いる請求項１９から３２のいずれか一項に記載のサーバシステム（１）。

【請求項３４】

前記サーバのうち１つまたは複数はプログラム可能なデータベースを備える請求項１９から３３のいずれか一項に記載のサーバシステム（１）。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、電子メッセージの拡散を減少させる方法およびシステムに関する。より詳しくは、本発明は、サーバシステムにおいて歓迎しない電子メッセージの拡散を減少させる方法およびシステムに関し、前記サーバシステムは、前記電子メッセージを配送する１つまたは複数のサーバと、前記サーバシステムから前記電子メッセージを受信するように構成された少なくとも第１ユーザ機器および第２ユーザ機器とを備える。

【背景技術】

【０００２】

電子メールスパムは、一般に、電子メールの受信者によって受信される歓迎しない、かつ／または、望まない電子メールメッセージとして定義されうる。

【０００３】

電子メールスパムメッセージの量は、この１０年にわたって劇的に増加した。その理由は、ごくわずかのコストで電子メールを用いて届けることができる膨大な数の受取人に見出すことができる。電子メールの強制的な配送とこの要因の組み合わせは、電子メール、または、より一般に、電子メッセージングを、様々な商品およびサービスの広告のための魅力的な通信媒体にした。世界中の人々の電子メールアドレスの収集は、たいへん低いコストで非常にたくさんの関係者から購入することができる。電子メールスパムメッセージは、現在、インターネット上で送信される全ての電子メールメッセージの９０％以上を占める。結果として、電子的リソースがかなりの量まで浪費されている。

【０００４】

電子メールスパムメッセージの量の増加は、他者に電子メールスパムフィルタの提供を引き起こした。これらのフィルタは、サーバ側とクライアント機器側の両方にインストールして、ユーザを煩わせることなく電子メールスパムメッセージを検出および削除することができる。典型的に、これらのフィルタは、電子メールスパムを認識するために、電子メールメッセージを解析し、電子メールスパムルールに対して解析結果を合致させる。これらの電子メールスパムルールは、電子メールヘッダの受取人の数、または、電子メール本体のある語句の出現のような、電子メールスパムメッセージの知られた典型的な特性に基づいて設計されている。

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかし、新たな形態のスパムは、これらの新たな形態の電子メールスパムメッセージのためのこれらのスパムルールをその時までにスパムフィルタに実装できないため、電子メールスパムルールはこれらの新たな形態のスパムを認識することができないので、これらのフィルタによって認識され、阻止されるとは限らない。その結果、電子メールスパムを行う者とスパムフィルタの供給者の間で絶え間のない競争が存在し、明らかに後者は前者に遅れをとる。一方、電子メールメッセージは、スパムフィルタの電子メールスパムルールの集合によって指図されるようにスパムとみなされるので、歓迎し、望まれる電子メールメッセージは、時々、受信者の電子メールボックスからフィルタリングされる。

【０００６】

さらに、電子メールスパムフィルタがインストールされているならば、フィルタは、電子メールスパムメッセージを検出するために個々の電子メールメッセージを解析する。その結果、メッセージ伝送は遅延し、リソースが浪費される。

【０００７】

米国特許出願公開第２００７／０１０６７３４号明細書は、望まない電子メッセージの拡散を制限する、サーバを備えるシステム、および、方法を開示している。そのサーバは、第１電子メッセージをスパムとして識別する第１ユーザから通知を受信し、第１電子メッセージと対応付けされるパラメータをスパム基準に対して比較することができる。スパム基準と合致するパラメータに応答して、第１電子メッセージの他のインスタンスが他のユーザに送信されることから阻止され、第１ユーザのアカウントについての信用通知を生成することができる。そのユーザからスパムが生じた第２ユーザは、第１ユーザの阻止される送信者リストに追加することができる。第１ユーザから第２ユーザへの生成された第２電子メッセージの識別に応答して、第１ユーザのアカウントについて訂正義務通知を生成することができる。

【０００８】

米国特許出願公開第２００７／０１０６７３４号明細書のシステムおよび方法は、スパムフィルタを使用し、スパムパラメータをスパム基準に対して照合する必要がある。スパムパラメータが識別されたときのみ、ユーザはスパム通知を送信し、他のインスタンスを

阻止することが可能である。
【０００９】
この技術分野において、電子メッセージ、特に、電子メールスパムメッセージの拡散を減少させるために、向上した、または、異なる方法およびシステムの必要性が存在することが明らかである。
【課題を解決するための手段】
【００１０】
本発明の目的は、上述した課題を低減させる方法およびシステムを提供することである。
【００１１】
この目的のために、電子メッセージを配送する１つまたは複数のサーバを備えるサーバシステムにおいて、電子メッセージの拡散を減少させる方法が提案される。前記方法は、少なくとも１つの電子メッセージまたはその一部を提供するステップと、前記電子メッセージまたはその一部に関する少なくとも１つのスパム通知信号を受信するステップと、を含む。電子メッセージの一部は、例えば、電子メッセージの１つまたは複数のフィールド、または、電子メッセージのフィールドまたは特性に基づいて組み立てられた新たな一部を含みうる。前記少なくとも１つのスパム通知信号の受信に応答して、電子メッセージ（および／またはその一部）、および／または、同じ送信元の他の（以前または将来の）電子メッセージへのアクセスが制限される。結果として電子メッセージへのアクセスの制限となるスパム通知信号の数を設定することが可能である。一例として、その数は、電子メッセージへのアクセスが制限される前に、５０、２５、１０、５、または、さらに、１つのスパム通知信号に設定することが可能である。
【００１２】
特に、前記サーバシステムは、前記サーバシステムから電子メッセージを受信するように構成された少なくとも第１ユーザ機器および第２ユーザ機器に接続するように構成されることが可能である。前記方法は、前記サーバシステムから前記第１ユーザ機器に少なくとも１つの電子メッセージを提供するステップを含む。その代わりに、電子メッセージの一部のみが第１ユーザ機器に送信される。サーバシステムは、続いて、電子メッセージが第１ユーザ機器のユーザによってスパムメッセージとして識別されたならば、電子メッセージまたはその一部に関するスパム通知信号を第１ユーザ機器から受信する。第１ユーザ機器からのスパム通知信号の受信に応答して、サーバシステムは、第２ユーザ機器またはユーザについて、電子メッセージおよび／またはその一部および／または同じ送信元からの他の電子メッセージへのアクセスを制限する。
【００１３】
また、出願人は、コンピュータプログラム、および、そのようなコンピュータプログラムを含む担体を提案し、そのコンピュータプログラムは、電子機器にインストールされ、電子機器によって実行されるとき、先の段落で説明した方法を実行することが可能なソフトウェアコード部分を含む。
【００１４】
また、サーバシステムは、電子メッセージの拡散を減少させるように構成された１つまたは複数のサーバを備えることを提案する。前記サーバシステムは、電子メッセージまたはその一部を受信するように構成された電子メッセージ受信部と、前記電子メッセージまたはその一部を提供するように構成された電子メッセージ提供部と、を備える。前記電子メッセージまたはその一部に関する少なくとも１つのスパム通知信号を受信するように構成されたスパム通知受信部が提供される。前記サーバシステムは、前記少なくとも１つのスパム通知信号の受信に応答して、前記電子メッセージ（および／またはその一部）および／または同じ送信元からの他の（以前または将来の）電子メッセージへのアクセスを制限するように構成されたアクセス制限部を備える。
【００１５】
特に、前記サーバシステムは、ネットワークを介して少なくとも第１および第２ユーザ

機器と通信するように構成される。前記電子メッセージ提供部は、前記電子メッセージまたはその一部を前記第１ユーザ機器に提供するように構成される。前記スパム通知受信部は、前記第１ユーザ機器からスパム通知信号を受信するように構成される。前記アクセス制限部は、前記第１ユーザ機器からの前記スパム通知信号の受信に応答して、前記第２ユーザ機器またはユーザについて、前記電子メッセージ（および／またはその一部）および／または同じ送信元からの他の（以前または将来の）電子メッセージへのアクセスを制限するように構成される。

【００１６】

電子メッセージ、その一部、または、他の以前または将来の電子メッセージへのアクセスは、ユーザ機器および／またはユーザ機器のユーザについて制限することが可能であり、後者の選択肢は、例えば、ユーザの識別データを利用することに留意すべきである。

【００１７】

また、サーバシステムは、必ずしもクライアントサーバシステムを指し示さないことを理解すべきである。また、本発明は、例えば、サーバまたは（いくつかの）サーバの機能がピアツーピアネットワークに参加するユーザ機器のうち１つまたは複数の一部であると考えられうるビットトレント（BitTorrent）アプリケーションのために使用されるようなピアツーピアネットワークに適用可能である。そして、スパム通知信号は、例えば、ピアツーピアネットワーク上で１つのユーザ機器から他へブロードキャストすることが可能である。

【００１８】

前記方法およびシステムは、ウェブアプリケーションとして実現することが可能である。

【００１９】

出願人は、先行技術の電子メールスパムフィルタの使用が不満足であると実感した。電子メールスパムメッセージを認識するために使用されるルール集合は、スパムフィルタの開発者によって提供されるルール集合の定期的な更新にもかかわらず、常に時期遅れである。結局、人間のみが電子メールスパムメッセージを認識することができる。さらに、出願人は、スパムフィルタの向上は、スパムを減少させるより、むしろスパムの全体の量の増加の一因となっていると実感した。従って、出願人は、ユーザからのスパム通知信号（のみ）を使用して電子スパムメッセージを検出し、そのようなスパム通知信号を受信すると、他のユーザ機器（のユーザ）について対応する電子メッセージへのアクセスを制限することを提案する。従って、サーバシステムは、電子メッセージの受取人自身が、どの電子メッセージがスパムメッセージであるか判定し、受取人は、続いて、そのメッセージ（および、一形態として、同じ送信元からの他の以前または将来の電子メッセージ）への他の受取人のアクセス（権）を決定することを可能とする。言い換えると、スパム通知信号は、メッセージへのアクセスを制限するサーバシステムへの指示である。複数のスパム通知信号の場合、各々の信号は部分的な指示とみなすことができる。一例として、他のユーザ機器（のユーザ）は、電子メッセージを表示またはダウンロードできない。スパム認識ルールの集合、スパムパラメータおよび基準を使用するスパムフィルタは、それらの電子メッセージについてスパム通知信号が受信された少なくともそれらの電子メッセージについて、サーバシステム内に存在しないことが可能である。

【００２０】

請求項３、４、および、２４の実施形態は、電子メッセージ配送のための加入者のみのシステムを確立する効果を与える。加入者は知られているので、電子メールスパムを行う者、および、他のシステムの悪用者を特定し、システムに加入者として参加することから排除することができる。さらに、この実施形態は、サーバシステムのユーザの識別が、システムからユーザを排除することを可能とする。

【００２１】

請求項５および２５の実施形態は、システムへの参加者の身元をかぎつけ、続いて、虚偽の身元によってサーバシステムに参加する可能性を阻止する。データを暗号化し、また

は、安全なネットワーク接続を提供するような、１つまたは複数の知られた技術によって安全な通信を実現することが可能である。

【００２２】

従来の電子メールサーバは、各々の受取人について電子メールメッセージを重複させる。重複した電子メールメッセージは、各々、従来のスパムフィルタによって解析される。請求項６から１０および２６から３０の実施形態は、制限されたリソースの使用の効果を与える。また、この実施形態は、電子メッセージへのアクセス制限を容易にする。これらの実施形態において、元の電子メッセージを特徴付けるほんの小さい部分（例えば、２００バイトまたは１００バイトより小さい）が受取人に入手可能にされる。これらの部分は、例えば、送信者の識別情報、電子メッセージの表題、電子メッセージの日付、および／または、完全な電子メッセージをどこで、および／または、どのように取得すべきかの情報を含む取得キーを含むことが可能である。電子メッセージの部分は、サーバシステムのサーバにプッシュされるか、または、必要ならば、サーバシステムの特定のサーバから照会されることが可能である。従って、リソースを消費する処理およびネットワーク容量の要求条件が著しく低減される。本願と同日に出願された出願人の同時係属中の国際特許出願（“Method and system for transmitting an electronic message”（電子メッセージを送信する方法およびシステム））への参照が行われ、その国際特許出願の内容は、その全体を引用して本願に組み込まれる。

【００２３】

請求項１１から１３および３１から３３の実施形態は、その電子メッセージについてスパム通知信号が受信された電子メッセージの送信者識別情報に基づいて、同じ送信元からの他の以前および／または将来の電子メッセージへのアクセスをユーザが制限することを可能とする効果を与える。送信者の攻撃の数のような各種のパラメータに基づいて、送信者についてのそのような手段の厳格さを軽減するために用意をすることができる。特に、出願人は、送信者と、その受取人からスパム通知信号が受信された１または複数の受取人との間の通信履歴に応じて、その電子メッセージについて少なくとも１つのスパム通知信号が受信された電子メッセージの受取人について他の電子メッセージへのアクセスを制限することを提案する。一例として、他の電子メッセージへのアクセス制限は、送信者が受信者に知られていない（例えば、送信者と受信者が以前に電子メッセージを交換していない）ならば即座に実行することが可能である。しかし、送信者と受信者が互いを知っているならば、他の電子メッセージへのアクセスはすぐには制限されない（しかし、一形態として、異なる電子メッセージについていくつかのスパム通知信号が受信された後にのみ制限される）。

【００２４】

請求項１４および３４の実施形態は、電子スパムメッセージ、および／または、送信されたその一部で、それらについての受取人であるユーザ機器の各々のユーザを煩わせないことを可能とする。

【００２５】

請求項１５および３５の実施形態は、サーバシステムが、その電子メッセージについてスパム通知信号が受信された電子メッセージの送信者に警告信号を送信することを可能とする。これは、さらなる攻撃の結果に関する情報を送信者に提供することを可能とする。サーバシステムへのアクセスを制限する結果は、請求項１６、１７、３６、および、３７の実施形態によって得ることができる。もはやサーバシステムへのアクセスを与えない結果は軽減することが可能である。特に、出願人は、送信者と、その受取人からスパム通知信号が受信された１または複数の受取人との間の通信履歴に応じて、その電子メッセージについて少なくとも１つのスパム通知信号が受信された電子メッセージの送信者について、サーバシステムへのアクセスを制限することを提案する。一例として、送信者が受信者に知られておらず（例えば、送信者と受信者が以前に電子メッセージを交換していない）、かつ、受信者がスパム通知信号を送出するならば、サーバシステムへのアクセス制限は即座に実行することが可能である。しかし、送信者と受信者が互いを知っているならば、

サーバシステムへのアクセスは、知られている受信者のユーザ機器から送出されたスパム通知信号に応答して即座には制限されない（しかし、一形態として、異なる電子メッセージについてスパム通知信号が受信された後にのみ制限される）。本願と同日に出願された出願人の同時係属中の国際特許出願（“Method and system for restricting access to an electronic message system”（電子メッセージシステムへのアクセスを制限する方法およびシステム））への参照が行われ、その国際特許出願の内容は、その全体を引用して本願に組み込まれる。

【００２６】

もちろん、サーバシステムは、電子メッセージの拡散を減少させるために、本願で説明される機能に加えてスパムフィルタを利用することが可能である。しかし、上記で定義されているようなサーバシステムは、請求項１８および３８において定義されているように、これらの可能なスパムフィルタの動作とは関係なく動作する。

【００２７】

請求項１９および３９の実施形態は、前もって電子メッセージの交換のための承認を可能とする。承認モジュールは、電子メッセージの受取人を指定するためにユーザが使用すべき必須のアドレス帳と組み合わせることが可能である。

【００２８】

本発明の一実施形態において、サーバシステムは電子メールサーバを備えていない。電子メールサーバは、典型的に、電子メッセージを記憶し、要求時にそのメッセージを転送するのみである。請求項４０の実施形態は、プログラム可能なデータベースを使用することを提案する。プログラム可能なデータベースは、受信された要求の種類に応じて予め定められた応答をプログラムすることを可能とする。スパム通知について、ユーザはデータベース上で動作（要求）を実行することが可能とされ、データベースの応答は、例えば、電子メッセージの他の受取人についてのアクセスの制限、同じ送信元の他の電子メッセージへのアクセスの制限、および／または、システムからの送信者の排除である。さらに、そのようなプログラム可能なデータベースは、いくつかのパラメータの間の関係を監視することを可能とする。

【００２９】

また、出願人は、ソフトウェアコード部分を有するユーザ機器、および、上述した方法の１つまたは複数のステップを実行し、かつ／または、上述したサーバシステムと通信するためのソフトウェアコード部分を有するコンピュータプログラムを提案する。

【００３０】

また、出願人は、サーバシステムおよび第１および第２ユーザ機器を備える、電子メッセージを交換する通信システムを提案する。

【００３１】

さらに、出願人は、請求項４４から６３で定義されているような情報交換システムを提案する。

【００３２】

上記実施形態またはその態様は、組み合わせ、または、分離することが可能であることに留意すべきである。一例として、前記方法およびサーバシステムは、また、他の以前または将来の電子メッセージのみ、すなわち、その電子メッセージについて１つまたは複数のスパム通知信号が受信された特定の電子メッセージへのアクセスを制限することなく、アクセスを制限することを可能とする。言い換えると、請求項１１から１３および３１から３３で定義されているような方法およびシステムは、それぞれ、請求項１および２２の構成と関係なく適用することが可能である。

【００３３】

以下、本発明の実施形態をさらに詳細に説明する。しかし、これらの実施形態は、本発明の保護範囲の限定と解釈されないことを理解すべきである。

【図面の簡単な説明】

【００３４】

【図１】電子メッセージを交換する通信システムの例を表わす図である。
【図２】サーバシステムの例を表わす図である。
【図３】図１の通信システムのための電子メッセージの拡散を減少させる方法のステップを表わすフローチャートを表わす。
【図４】電子メッセージを交換する通信システムのもう１つの例を表わす。
【図５】図４の通信システムのための電子メッセージの拡散を減少させる方法のステップを表わすフローチャートを表わす。
【図６】本発明の一実施形態によるサーバシステムのサーバのデータベースのための例示のモデルを表わす。
【発明を実施するための形態】
【００３５】
図１および図２は、本発明の一実施形態によるサーバシステム１を表わす。サーバシステム１は、ネットワーク接続２を介して第１ユーザ機器Ｉ、第２ユーザ機器ＩＩ、および、第３ユーザ機器ＩＩＩに接続されている。ネットワーク接続２は、有線および無線の両方の複数のネットワークを含み、ユーザ機器Ｉ、ＩＩ、ＩＩＩの接続は、必ずしもサーバシステム１に直接ではない。
【００３６】
第１、第２、および、第３ユーザ機器Ｉ、ＩＩ、ＩＩＩは、電子メールメッセージのような電子メッセージを送信および受信するように構成されており、パーソナルコンピュータ、携帯通信機器等でありうる。
【００３７】
サーバシステム１は、プロセッサ１０、メモリ１１、および、第１、第２、および、第３ユーザ機器Ｉ、ＩＩ、ＩＩＩと通信するためのネットワークアダプタ１２を備える。サーバシステム１は、通常、図１に表わされている３つのユーザ機器Ｉ、ＩＩ、および、ＩＩＩより多くに接続可能であることを理解すべきである。
【００３８】
サーバシステム１の具体的な機能が図２に図式的に表わされており、ここでより詳細に説明する。その機能は、大部分は、プロセッサ１０によって実行される１つまたは複数のコンピュータプログラムのソフトウェアコード部分として実現されうることを理解すべきである。
【００３９】
サーバシステム１は、第３ユーザ機器ＩＩＩから電子メッセージを受信するように構成されている。
【００４０】
サーバシステム１は、電子メッセージまたはその一部を受信するように構成された電子メッセージ受信部１３、当該電子メッセージまたはその一部を第１ユーザ機器Ｉに提供するように構成された電子メッセージ提供部１４を備える。また、サーバシステム１は、第１ユーザ機器Ｉから電子メッセージまたその一部に関するスパム通知信号を受信するように構成されたスパム通知受信部１５を含む。また、サーバシステム１は、第１ユーザ機器からのスパム通知信号の受信に応答してのみ、第２ユーザ機器ＩＩ（のユーザ）について電子メッセージへのアクセスを制限するように構成されたアクセス制限部１６を備える。
【００４１】
サーバシステム１は、ユーザ機器Ｉ、ＩＩ、および、ＩＩＩの各ユーザについてサーバシステム１にアクセスするために必要なユーザ名およびユーザ固有のパスワードを含むユニークなログインコードを記憶するレジスタ１７を有する。
【００４２】
ネットワーク接続２における通信は安全にされる。この目的のために、サーバシステム１は、サーバシステム１と、第１、第２、および、第３ユーザ機器Ｉ、ＩＩ、および、ＩＩＩとの間の一部または全部の通信を暗号化する暗号部１８を含む。その代わりに、または、それに加えて、ネットワーク接続２を安全にすることが可能であることに留意すべき

である。安全な通信は、第１、第２、および、第３ユーザ機器Ｉ、ＩＩ、および、ＩＩＩ（のユーザ）の身元をかぎつける可能性を阻止または減少させる。

【００４３】

サーバシステム１は、第１ユーザ機器Ｉおよび第２ユーザ機器ＩＩの両方について電子メッセージの複製を作成するように構成することが可能である。しかし、サーバシステム１は、第３ユーザ機器ＩＩＩから受信された電子メッセージの１つの複製のみを記憶することも可能である。

【００４４】

サーバシステム１は、第１ユーザ機器Ｉからのスパム通知信号に応答して、電子メールおよび複製および／または存在すればその一部を削除する電子メール削除部１９を有する。

【００４５】

さらに、サーバシステム１は、スパム通知信号受信部１５が、その電子メッセージについてスパム通知信号を受信した電子メッセージの送信者の送信者識別情報、すなわち、第３ユーザ機器ＩＩＩのユーザの識別情報を記憶するように構成された送信者識別情報記憶部２０を有する。他の電子メッセージが受信され、または、このユーザから過去に受信されたならば、アクセス制限部１６は、送信者の識別情報を使用して、自動的に、すなわち、これらの他の電子メッセージについてのさらなるスパム通知信号を要求することなく、第２ユーザ機器ＩＩについてこれらの他の電子メッセージへのアクセスを制限することが可能である。もちろん、アクセス制限は、第１ユーザ機器（のユーザ）について適用することも可能である。

【００４６】

アクセス制限部１６は、例えば、第２ユーザ機器ＩＩ（のユーザ）について、特定の期間に、または、他の電子メッセージの一部に、アクセスが制限されるように構成することが可能である。しかし、アクセス制限部１６は、第２ユーザ機器への電子メッセージのダウンロードを阻止し、または、第２ユーザ機器ＩＩにおける電子メッセージの表示を阻止することも可能である。

【００４７】

特に、送信者と、その受信者からスパム通知信号が受信された受信者との間の通信履歴を考慮することが可能である。例えば、第３ユーザ機器ＩＩＩおよび第１ユーザ機器Ｉのユーザが以前に電子メッセージ交換をしていない（すなわち、これらのユーザは互いを‘知らない’）ならば、スパム通知信号の受信は、他の受取人が他の過去および将来の電子メッセージをダウンロードまたは表示することを即座に阻止する結果になりうる。しかし、第３ユーザ機器ＩＩＩおよび第１ユーザ機器Ｉのユーザが過去に電子メッセージ交換をした（すなわち、これらのユーザは互いを‘知っている’）ならば、スパム通知信号の結果はあまり厳格でなくてもよい。互いを‘知っている’ユーザのもう１つの例は、各々のユーザが、電子メッセージの交換に先立って互いからの電子メッセージを受け取ることを知らせたことでありうる。

【００４８】

サーバシステム１は、特定の送信者の電子メッセージについて受信されたスパム通知信号の数をカウントし、かつ／または、送信者の電子メッセージについてアクセスが制限された回数をカウントするように構成されたカウンタ２１を含むことが可能である。

【００４９】

サーバシステム１は、その電子メッセージについて第１ユーザ機器Ｉからスパム通知信号が受信された電子メッセージの送信者に警告メッセージを送信するように構成された警告メッセージ送信部２２を備える。

【００５０】

また、サーバシステム１は、その電子メッセージについてスパム通知信号が受信された電子メッセージの送信者、すなわち、第３ユーザ機器ＩＩＩを使用する送信者についてサーバシステム１へのアクセスを制限するように構成されたアクセス制限部２３を備える。

アクセスの制限は、サーバシステム１を介した電子メッセージのさらなる送信および／または受信から第３ユーザ機器ＩＩＩのユーザを排除することを含みうる。しかし、サーバシステム１は、例えば、送信者の電子メッセージについて受信されたスパム通知信号の数、および／または、送信者の電子メッセージについてアクセスが制限された回数に応じて、サーバシステムへのアクセスを制限するように構成された評価モジュール２４を備えることが可能である。

【００５１】

特に、送信者と、その受信者からスパム通知信号が受信された受信者との間の通信履歴を考慮することが可能である。例えば、第３ユーザ機器ＩＩＩおよび第１ユーザ機器Ｉのユーザが以前に電子メッセージ交換をしていない（すなわち、これらのユーザは互いを‘知らない’）ならば、スパム通知信号の受信は、送信者についてサーバシステム１へのアクセスを即座に阻止する結果になりうる。しかし、第３ユーザ機器ＩＩＩおよび第１ユーザ機器Ｉのユーザが過去に電子メッセージ交換をした（すなわち、これらのユーザは互いを‘知っている’）ならば、スパム通知信号の結果は、第３ユーザ機器ＩＩＩのユーザについてあまり厳格でなくてもよい。互いを‘知っている’ユーザのもう１つの例は、各々のユーザが、電子メッセージの交換に先立って互いからの電子メッセージを受け取ることを知らせたことでありうる。

【００５２】

サーバシステム１は、電子スパムメッセージを検出して、一形態として、それへのアクセスを制限するために、スパムルールの集合、スパムパラメータ、および、スパム基準を使用するスパムフィルタを含むことが可能であることに留意すべきである。しかし、サーバシステム１は、スパムフィルタの動作とは関係なく、すなわち、スパム通知信号のみに基づいて、第２ユーザ機器ＩＩ（のユーザ）および／または電子スパムメッセージの送信者についてサーバシステム１へのアクセスを制限することが可能である。

【００５３】

最後に、サーバシステム１は、送信者と受取人の両方が事前に承認モジュール２５に交換についての承認を知らせた場合のみ、送信者、例えば第３ユーザ機器ＩＩＩのユーザと、受取人、例えば第１ユーザ機器Ｉのユーザとの間での電子メッセージの交換を可能とするように構成された承認モジュール２５を含む。電子メッセージを送信および受信するためにユーザ機器ＩおよびＩＩＩにおいて動作するコンピュータプログラムは、例えば、承認モジュール２５の制御のもとで必須のアドレス帳を備えることが可能である。このアドレス帳を使用することによってのみ、送信者は電子メッセージの受取人をアドレス指定することが可能である。アドレス帳のエントリは、電子メッセージを交換するユーザの相互の承認に応答してのみ作成することができる。

【００５４】

図３は、本発明の一実施形態によるサーバシステム１の動作のいくつかのステップを含むフローチャートを表わす。

【００５５】

最初のステップ３０において、サーバシステム１の電子メッセージ受信部１３は、第３ユーザ機器ＩＩＩから、安全なネットワーク接続２上で、特に、ユーザ機器ＩおよびＩＩのユーザに送信された電子メッセージを受信する。ステップ３１において、サーバシステム１の電子メッセージ提供部１４は、電子メッセージを第１ユーザ機器Ｉに提供する。

【００５６】

最初の読者、例えば、第１ユーザ機器Ｉのユーザは、その電子メッセージを望ましいメッセージとして受け取り、その電子メッセージに関してサーバシステム１によってスパム通知信号は受信されない。従って、ステップ３２に示されているように、第２ユーザ機器ＩＩのユーザはその電子メッセージにアクセスすることが可能である。

【００５７】

第１ユーザ機器Ｉのユーザがその電子メッセージの内容をスパムとみなしたならば、彼は電子スパムメッセージに関するスパム通知信号をサーバシステム１に送信することが可

能である。第１ユーザ機器Ｉのユーザは、例えば、第１ユーザ機器Ｉのユーザインタフェース上の専用ボタンを動作させることによってスパム通知信号を送信することが可能である。スパム通知信号は、サーバシステム１のスパム通知信号受信部１５によって検出される。スパム通知応答信号の受信に応答して、アクセス制限部１６は、ステップ３３に示されているように、第２ユーザ機器ＩＩ（のユーザ）についてその電子メッセージへのアクセスを制限する。サーバシステム１の電子メール削除部１９は、例えば、その電子スパムメッセージについてスパム通知信号が受信された電子スパムメッセージを削除することが可能である（ステップ３４）。

【００５８】

好ましくは、電子スパムメッセージを配送する第３ユーザ機器ＩＩＩのユーザは、例えば、サーバシステム１にアクセスするために必要なユーザ名およびユーザ固有のパスワードを含むユニークなログインコードをレジスタ１７に記憶させることによって、サーバシステム１に知られている。これらのデータを使用して、送信者識別情報記憶部は電子スパムメッセージの送信者の識別情報を記憶している。他の電子メッセージ（必ずしも電子スパムメッセージではない）が送信され、または、以前に送信されたならば、この送信者について、以前のスパム通知信号が既に受信されたと判定される。従って、送信者のこれらの他のメッセージへのアクセスが同様に拒否されうる。従って、第１ユーザ機器Ｉおよび第２ユーザ機器ＩＩのいずれも、これらの他の電子メッセージへのアクセスを有さない（ステップ３５）。そのような手段は以前の電子スパムメッセージの送信者にむしろ厳格でありうるので、アクセス制限部１６が、第２ユーザ機器ＩＩ（のユーザ）について、特定の期間に、かつ／または、他の電子メッセージの一部のみに、アクセスを制限することを可能とすることによって結果を軽減することが可能である。この目的のために評価モジュール２４を使用することが可能である。特に、送信者および受信者が以前に電子メッセージを交換したならば、他の電子メッセージへのアクセス制限は、カウンタ２１を使用して、受信者からのスパム通知信号がある数を超えた場合のみ実行されることが可能である。

【００５９】

最後に、ステップ３６において、アクセス制限部２３は、そのユーザ機器についてスパム通知信号が受信された第３ユーザ機器ＩＩＩ（のユーザ）についてサーバシステム１へのアクセスを制限する。アクセスの制限は、第３ユーザ機器ＩＩＩのユーザが、サーバシステム１を介して電子メッセージをさらに送信および／または受信することを排除することを含みうる。再び、そのような手段は、第３ユーザ機器ＩＩＩのユーザに厳格でありうるので、評価モジュール２４は、例えば、送信者の電子メッセージについて受信されたスパム通知信号の数、および／または、送信者の電子メッセージについてアクセスが制限された回数に応じて、サーバシステム１へのアクセスを制限することが可能である。特に、送信者および受信者が以前に電子メッセージを交換したならば、サーバシステムへのアクセス制限は、カウンタ２１を使用して、受信者からのスパム通知信号がある数を超えた場合のみ実行されることが可能である。

【００６０】

上記の例において、他の受取人が（他の）電子メッセージを受信することを排除し、送信者がシステムに関与することを排除するために、１つのスパム通知信号が十分であり、そのような結果を適用する前に、他の数のスパム通知信号を設定することが可能であることを理解すべきである。

【００６１】

図１のシステムにおいて、サーバシステム１は１つのサーバを備える。しかし、図４に表わされているように、サーバシステム１は、互いと通信接続するいくつかのサーバ１Ａ、１Ｂ、１Ｃを備えることも可能である。すなわち、サーバ１Ａ、１Ｂ、および、１Ｃは、一緒にサーバシステム１を構成する。サーバ１Ａ、１Ｂ、および、１Ｃを接続する接続４０は、内側のリングを構成する。第１、第２、および、第３ユーザ機器Ｉ、ＩＩ、および、ＩＩＩは、図４に表わされているように、この内側のリングの個々のサーバ１Ａ、１Ｂ、および、１Ｃに、直接に、または、（図示しない）さらなるサーバを介して、接続す

ることが可能である。また、第１、第２、および、第３ユーザ機器Ｉ、ＩＩ、および、ＩＩＩの各々は、接続４０によって構成された内側のリングを使用することなく、それぞれ、サーバ１Ｂと１Ｃ、１Ａと１Ｃ、１Ａと１Ｂにアクセスすることが可能である。図４において、接続４１によって構成されるこの外側のリングは、第１ユーザ機器Ｉについてのみ表わされている。

【００６２】

内側のリングおよび外側のリングの両方において通信を安全にすることが可能である。これは、内側のリングおよび外側のリングにわたって通信を暗号化することによって、かつ／または、安全な接続を利用することによって行うことが可能である。

【００６３】

サーバシステム１の各サーバ１Ａ、１Ｂ、１Ｃは、図２を参照して説明したのと同じ機能モジュール１３～２５を含むことが可能である。しかし、機能モジュールは、各種のサーバ１Ａ、１Ｂ、および、１Ｃにわたって分散することも可能である。

【００６４】

ここで、図５を参照して、図４によるシステムの動作の一実施形態を説明する。

【００６５】

第３ユーザ機器ＩＩＩのユーザは、受取人としてユーザ機器ＩおよびＩＩのユーザを有する電子スパムメッセージをサーバシステム１に送信する。

【００６６】

図６を参照してさらに説明するように、ステップ５０において、サーバ１Ｃの電子メッセージ受信部１３は、電子スパムメッセージを受信し、一形態として、フィールドに区分し、メモリ１１にメッセージ／フィールドを記憶する。簡潔には、従来の電子メールサーバに電子メッセージを記憶する代わりに、電子メッセージの個々の部分（フィールド）が、データベースモデルのフィールドに別個に記憶される。

【００６７】

ステップ５１において、第３サーバ１Ｃの電子メッセージ提供部１４は、元の電子メッセージの特性を用いて電子メッセージの一部を組み立てる。電子メッセージの一部は、例えば、電子メッセージの１つまたは複数のフィールド、または、電子メッセージの特性に基づいて組み立てられた新たな一部を含みうる。一例として、電子メッセージの一部は、送信者フィールド、表題フィールド、完全な電子メッセージを取得するための取得キー、および、一形態として、日付を含む。電子メッセージの一部のデータサイズは、２００バイトより小さいことが可能である。電子メッセージ提供部１４の部分提供部は、サーバシステム１の内側のリングを使用して、電子メッセージの一部を第１サーバ１Ａおよび第２サーバ１Ｂに送信する。第３サーバ１Ｃから第１および第２サーバ１Ａ、１Ｂに電子メッセージの一部をプッシュする代わりに、第１サーバ１Ａは、第１ユーザ機器Ｉからメールボックスを開く要求を受信すると、第３サーバ１Ｃから電子メッセージの一部を照会することが可能である。本願と同じ出願人による、本願と同日に出願された国際特許出願（“Method and system for transmitting an electronic message”（電子メッセージを送信する方法およびシステム））への参照が行われ、その国際特許出願の内容は、その全体を引用して本願に組み込まれる。この後者の代替は、さらに、必要ならば電子メッセージの小さな部分のみが伝送される効果を与える。完全な電子メッセージはサーバ１Ｃにのみ記憶される。

【００６８】

再び、第１ユーザ機器Ｉのユーザが、まず彼のメールボックスを開けると仮定する。それを行うことによって、ステップ５２において、第１サーバ１Ａは、電子メッセージの一部を第１ユーザ機器Ｉに提供する。ステップ５３において、第１サーバ１Ａから提供される電子メッセージの一部を選択することによって、外側のリングを構成する接続４１上で第３サーバ１Ｃから第１ユーザ機器Ｉによって電子メッセージそれ自体を取得することが可能である。

【００６９】

第１ユーザ機器Ｉのユーザがその電子メッセージをスパムとみなさないならば、第２ユーザ機器ＩＩのユーザは、例えば、第３サーバ１Ｃからその電子メッセージをダウンロードすることによって、その電子メッセージにアクセスすることが可能である（ステップ５４）。

【００７０】

第１ユーザ機器Ｉのユーザがその電子メッセージの内容をスパムとみなすならば、彼は電子スパムメッセージに関するスパム通知信号をサーバシステム１に送信することが可能である。第１ユーザ機器Ｉのユーザは、例えば、第１ユーザ機器Ｉのユーザインタフェース上の専用ボタンを動作させることによってスパム通知信号を送信することが可能である。スパム通知信号は、サーバ１Ｃのスパム通知信号受信部１５によって検出される。ステップ５５に示されているように、スパム通知信号の受信に応答して、サーバ１Ｃのアクセス制限部１６は、第２ユーザ機器ＩＩ（のユーザ）についてその電子メッセージへのアクセスを制限する。サーバ１Ｃの電子メール削除部１９は、例えば、第２ユーザ機器ＩＩのユーザが第３サーバ１Ｃにおいて電子スパムメッセージへのアクセスを有さないように、第２サーバ１Ｂにおいて電子スパムメッセージの一部を削除することが可能である。さらに、電子メール削除部１９は、第１サーバ１Ａからの電子メッセージの一部とともに、第３サーバ１Ｃのメモリ１１から電子スパムメッセージそれ自身を削除することが可能である。これらの手段は、ステップ５６および５７に示されている。電子メッセージ（の部分）の削除は、図４の内側のリングを介して指示される。

【００７１】

上述したように、サーバシステム１は、受取人の数に関係なく、（サーバ１Ｃにおいて）電子メッセージの１つの複製のみを記憶する。受取人は、小さいサイズの電子メッセージを特徴付ける部分によって電子メッセージが通知される。これは大量のリソースを節約する。しかし、サーバシステム１は、そのようなアプローチがより効果的であることが証明されるならば、電子メッセージの複数の複製を提供することが可能である。電子メッセージの複製の数は、電子メッセージの受取人の数より小さい。

【００７２】

図１および図３の実施形態に関して、電子スパムメッセージを配送する第３ユーザ機器ＩＩＩのユーザは、例えば、サーバシステム１にアクセスするために必要なユーザアドレスおよびユーザ固有のパスワードを含むユニークなログインコードを第３サーバ１Ｃのレジスタ１７に記憶させることによって、サーバシステム１に知られうる。これらのデータを使用して、送信者識別情報記憶部２０は、電子スパムメッセージの送信者の識別情報を記憶している。他の電子メッセージ（必ずしも電子スパムメッセージではない）が送信される、または、送信されたならば、この送信者について以前のスパム通知信号が既に受信されたと判定される。従って、送信者のこれらの他のメッセージへのアクセスが機器ＩおよびＩＩの両方のユーザについて拒否されうる。従って、第１ユーザ機器Ｉおよび第２ユーザ機器ＩＩのいずれも、これらの他の電子メッセージへのアクセスを有さない。そのような手段は、以前の電子スパムメッセージの送信者にむしろ厳格でありうるので、第３サーバ１Ｃにおけるアクセス制限部１６が、第２ユーザ機器ＩＩ（のユーザ）について、特定の期間に、および／または、他の電子メッセージの一部のみにアクセスを制限することを可能とすることによって、結果を軽減することが可能である。特に、結果を決定するために、送信者についての通信履歴を使用することが可能である。

【００７３】

以前の電子スパムメッセージの送信者のための送信者識別情報記憶部２０とともに、複数のサーバ１Ａ、１Ｂ、および、１Ｃによってレジスタ１７を共有することが可能であることを理解すべきである。

【００７４】

また、図１および図３の実施形態について前述したように、サーバシステム１が、スパム通知信号を使用して、第３ユーザ機器のユーザについてサーバシステム１へのアクセスを阻止し（より緩やかな変形を含む）、または、警告メッセージを送信することを引き起

こすことが可能である。

【００７５】

再び、上記の例において、他の受取人が（他の）電子メッセージを受信することを排除し、送信者がシステムに関与することを排除するために、１つのスパム通知信号が十分であったが、そのような結果を適用する前に、他の数のスパム通知信号を設定することが可能であることを理解すべきである。

【００７６】

サーバシステム１のサーバ１Ａ、１Ｂ、および、１Ｃは、好ましくは、従来の電子メールサーバではない。そのような電子メールサーバは、電子メールメッセージを記憶し、電子メールメッセージを受取人の数だけ重複させ、それらのメッセージのうち特定の１つが要求されたときに電子メールメッセージを提供する。これらのメールサーバの機能はむしろ限られている。

【００７７】

出願人は、例えば、データベースに行われる要求に応じて応答をプログラムすることができる、オラクル（登録商標）データベースのような１つまたは複数のデータベースを使用することを提案する。入ってくる電子メッセージは、予め定められた部分において解析または受信され、データベースのフィールドに格納される。一例として、従来の電子メールのヘッダが別個のフィールドに格納され、そのいくつかが図６のデータモデルに表わされている。

【００７８】

上述した方法は、加入者のみのシステムにおいて実行することが可能であり、加入者／参加者の詳細が知られており、加入者は特定の全般的な条件に従うことに同意している。システムの会員は、図６のデータモデルにおいて場所を有する。

【００７９】

サーバ１Ａ、１Ｂ、および、１Ｃのためのデータベースの使用は、図６に表わされているように、個々のフィールド間の関係を監視することを可能とする。

【００８０】

上述した機能は、図６のデータベースモデルを使用して実現することができる。

【００８１】

一例として、ユーザがスパム通知信号を送出したならば、Recipient status（送信者状態）およびRecipient status date（受信者状態日付）が更新される。他の受信者について電子メッセージへのアクセスを制限し、送信者についてサーバシステム１へのアクセスを制限するために１つのスパム通知信号が十分であるならば、この状態は、それぞれ、Message status（メッセージ状態）およびMember status（会員状態）に伝播する。Message status date（メッセージ状態日付）およびMember status date（会員状態日付）をデータモデルに追加することによって、柔軟性が得られる。

【００８２】

“Messages”のボックスのフィールドは、サーバシステムにおいてプッシュ、または、照会される電子メッセージの一部とすることが可能である。例は、Message owner/sender（メッセージ所有者／送信者）、Message subject（メッセージ表題）、および、Message sent date（メッセージ送信日付）を含む。Message-id（メッセージ識別子）は、完全な電子メッセージを取得するための取得キーに関する。

【００８３】

電子メッセージの受取人をアドレス指定するための必須のアドレス帳が使用されないとき、“Contacts”のボックスはデータベースモデルから除去され、“Members”のボックスから“Recipients”のボックスへ直接にリンクを作成できることに留意すべきである。

【００８４】

サーバシステム１は承認モジュール２５を含むことが可能である。承認モジュールの下記で説明する動作は、特にスパム通知信号に関して、上述した方法と関係なく適用することが可能であることに留意すべきである。こうして、サーバシステム１は、全ての参加者

について参加者にアドレス指定された任意かつ全ての情報が到達できず、かつ、２人の参加者ＡとＢの間のシステム内での最初の通信に先立って、２人の参加者ＡとＢがまず取り決め／承認プロトコルを完了しなければならないように構成することが可能である。

【００８５】

ＡはＢとの通信を可能とするようにサーバシステム１に要求し、かつ、ＢはＡが要求を行ったときからカウントして予め定められた期間内に、例えば１日または２週間以内に、Ａとの通信を可能とするようにサーバシステム１に要求しないならば、サーバシステム１は、その通信をＢが望まないものとみなして登録し、取り決めプロトコルを打ち切る。

【００８６】

また、サーバシステム１は、参加者Ａが、予め定められた期間内に、例えば１日または２週間以内に、１回または複数回、例えば３回または１０回、１または複数の参加者Ｂ、Ｃ、等との通信を可能とするようにサーバシステム１に要求し、かつ、１または複数の参加者Ｂ、Ｃ、等が上記期間内にＡとの通信を可能とするようにサーバに要求しないならば、参加者Ａは望まない情報を拡散させる潜在的な送信元とみなされ、従って、サーバシステム１によるＡからの一方的な通信の要求の登録に基づいて、参加者Ａからの要求は管理者による厳密な検査を受けるように構成することが可能であり、この管理者は、例えばＡが電子スパムメッセージを送信するような有害な意図を有するように見えるならば、Ａの接続を停止することが可能である。

【００８７】

サーバシステム１は、ＡおよびＢが、１回のみ、または、特定の期間について、システムを介して、互いに情報をアドレス指定し、かつ／または、互いにダウンロードすることを可能とするように、ＡおよびＢが個々にサーバシステム１を設定することが可能であるように構成することが可能である。

【００８８】

サーバシステム１は、参加者Ａが、予め定められた期間内に、例えば１日または２週間以内に、繰り返し、例えば２回、システム内の他の参加者Ｂ、Ｃ、等に情報をアドレス指定し、かつ、Ａと他の参加者Ｂ、Ｃ、等との間で行われた通信の取り決めがこれを許容し、かつ、多数の参加者、例えば１または複数の参加者Ｂ、Ｃ、等が、固定された期間内にＡから生じる情報をそれ以上ダウンロードできないようにＡと行われた取り決めを制限するならば、管理者は、望まない通信の潜在的な送信元として参加者Ａを検出し、かつ、みなすように構成することが可能であり、この場合、参加者Ａからの通信の要求は管理者による厳密な検査を受け、この管理者は、例えばＡがスパムを送信するような有害な意図を有するように見えるならば、Ａの接続を停止することが可能である。

【００８９】

サーバシステム１は、１または複数の参加者Ｂ、Ｃ、等が、参加者Ａに関して行われた取り決めを、特定の期間、例えば１日または２週間について、Ａによってアドレス指定された情報をＢ、Ｃ、等がそれ以上ダウンロードできないように制限するならば、参加者Ａはサーバシステム１によって検出され、管理者によって望まない通信の潜在的な送信元とみなされるように構成することが可能であり、管理者は参加者Ａを望まない参加者として排除することができる。

【００９０】

また、サーバシステム１は、ボックス番号の所有者が参加者Ａに情報の送信を許可したボックス番号のうち１つ以外のボックス番号を参加者Ａがアドレス指定できないように構成することが可能である。

【００９１】

承認モジュール２５は、その変形において、電子メッセージの受取人をアドレス指定するための必須のアドレス帳と組み合わせて適用することが可能である。

【符号の説明】

【００９２】

１　・・・　サーバシステム

１Ａ、１Ｂ、１Ｃ　・・・　サーバ
２　・・・　ネットワーク接続
１０　・・・　プロセッサ
１１　・・・　メモリ
１２　・・・　ネットワークアダプタ
１３　・・・　電子メッセージ受信部
１４　・・・　電子メッセージ提供部
１５　・・・　スパム通知受信部
１６　・・・　アクセス制限部
１７　・・・　レジスタ
１８　・・・　暗号部
１９　・・・　電子メール削除部
２０　・・・　送信者識別情報記憶部
２１　・・・　カウンタ
２２　・・・　警告メッセージ送信部
２３　・・・　アクセス制限部
２４　・・・　評価モジュール
２５　・・・　承認モジュール
４０、４１　・・・　接続
Ｉ　・・・　第１ユーザ機器
ＩＩ　・・・　第２ユーザ機器
ＩＩＩ　・・・　第３ユーザ機器

【図１】

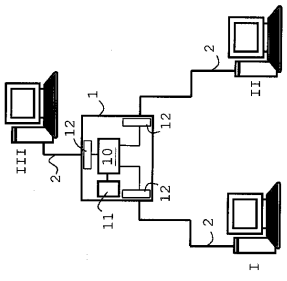


Fig. 1

【図２】

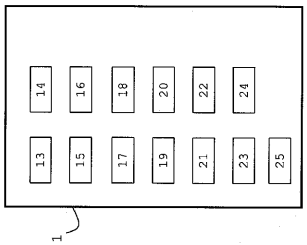
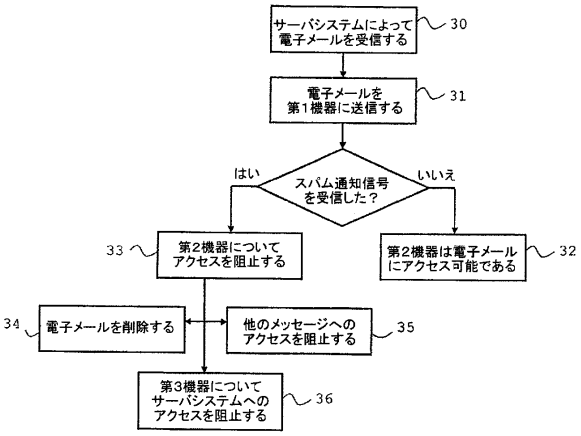


Fig. 2

【図３】



【図４】

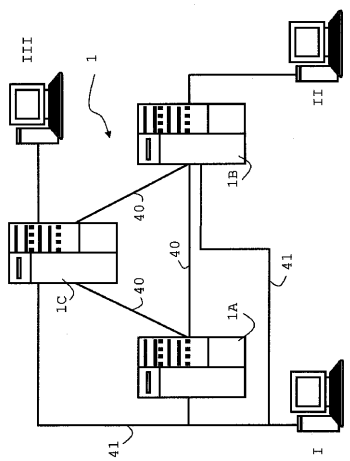
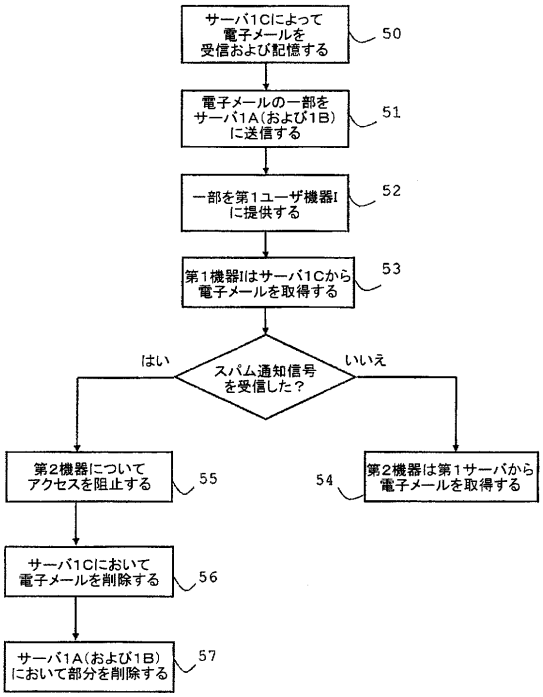


Fig. 4

【図５】



【図６】

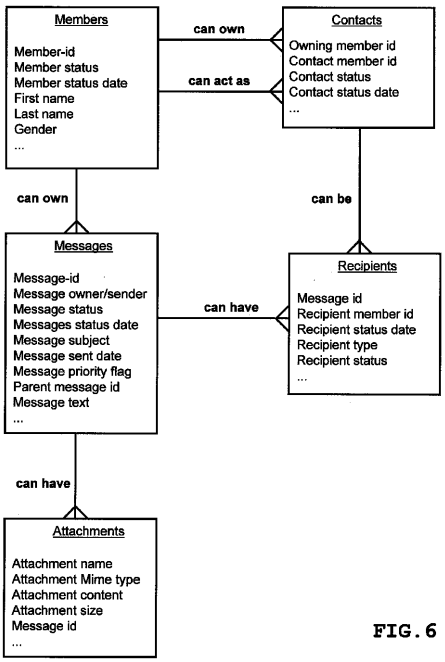


FIG.6

フロントページの続き

(72)発明者　ディルク・レオナルト・ベンショップ
オランダ・ＮＬ－４８７４・エルフェー・エテン－ルール・ラークセヴェク・２４
(72)発明者　ヘンデリック・レイナウト・ベンショップ
オランダ・ＮＬ－３１８１・エンエム・ローゼンブルク・スターボード・１６

審査官　速水　雄太

(56)参考文献　特開２００３－３４８１６２（ＪＰ，Ａ）
特開平１０－０７４１７２（ＪＰ，Ａ）
国際公開第０１／０７２００２（WO，Ａ２）
特開２００６－３１１６０７（ＪＰ，Ａ）
特開２００３－１６３６９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／５８