(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4537738号
(P4537738)
(45)発行日　平成22年9月8日(2010.9.8)　(24)登録日　平成22年6月25日(2010.6.25)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 610Q
H04L 12/58 (2006.01)　　H04L 12/58 100F

請求項の数 21　(全 42 頁)

(21)出願番号	特願2004-71769(P2004-71769)
(22)出願日	平成16年3月12日(2004.3.12)
(65)公開番号	特開2004-280827(P2004-280827A)
(43)公開日	平成16年10月7日(2004.10.7)
審査請求日	平成19年3月12日(2007.3.12)
(31)優先権主張番号	60/454,517
(32)優先日	平成15年3月12日(2003.3.12)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/684,020
(32)優先日	平成15年10月10日(2003.10.10)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/683,624
(32)優先日	平成15年10月10日(2003.10.10)
(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
(72)発明者　ロバート　ジョージ　アトキンソン
アメリカ合衆国　９８０７７　ワシントン州　ウッディンビル　ノースイースト　１９６　ストリート　１７９２６

最終頁に続く

(54)【発明の名称】不要メッセージおよび受信者側が送信を要求していないメッセージの低減のための方法及びコンピュータ可読媒体

(57)【特許請求の範囲】
【請求項１】
１つまたは複数の送信コンピュータシステムにネットワーク接続可能な受信コンピュータシステムであって、電子メッセージを前記送信コンピュータシステムから受信するように構成されている１つまたは複数の受信メッセージサーバを含む受信コンピュータシステムにおいて、送信コンピュータシステムの電子メッセージ送信ポリシーを判断するための方法であって、前記受信コンピュータシステムは、
前記送信コンピュータシステムからの電子メッセージを受信する動作と、
前記送信コンピュータシステムに対応する１つまたは複数の電子メッセージの送信ポリシーを受信する動作と、
前記１つまたは複数の受信電子メッセージ送信ポリシーから、関連電子メッセージ送信ポリシーを解析する動作と、
メッセージ分類モジュールが前記受信電子メッセージを分類する場合にさらに信頼性の高い決定を行うことが可能なように、前記関連電子メッセージ送信ポリシーを前記メッセージ分類モジュールに供給する動作とを実行することを特徴とする方法。
【請求項２】
前記送信コンピュータシステムから電子メッセージを受信する動作は、電子メールメッセージを受信する動作を含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記送信コンピュータシステムに対応する１つまたは複数の電子メッセージ送信ポリシ

ーを受信する動作は、前記受信電子メッセージに含まれる１つまたは複数の電子メッセージ送信ポリシーを受信する動作を含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記受信電子メッセージに含まれる１つまたは複数の電子メッセージ送信ポリシーを受信する動作は、１つまたは複数の電子メッセージ送信ポリシー証明書を受信する動作を含むことを特徴とする請求項３に記載の方法。
【請求項５】
前記１つまたは複数の電子メッセージ送信ポリシーを受信する動作は、前記１つまたは複数の電子メッセージ送信ポリシーの少なくとも１つについての新しさの証拠を受信する動作を含むことを特徴とする請求項４に記載の方法。
【請求項６】
前記受信電子メッセージに含まれる１つまたは複数の電子メッセージ送信ポリシーを受信する動作は、ＥＴＰ　Ｓ／ＭＩＭＥメッセージを受信する動作を含むことを特徴とする請求項３に記載の方法。
【請求項７】
前記ＥＴＰ　Ｓ／ＭＩＭＥメッセージを受信する動作は、証明書の新しさの証拠の指示を受信する動作を含むことを特徴とする請求項６に記載の方法。
【請求項８】
前記受信コンピュータシステムは、前記送信コンピュータシステムに対応する電子メッセージポリシーについてサーバに問い合わせる動作をさらに実行することを特徴とする請求項１に記載の方法。
【請求項９】
前記送信コンピュータシステムに対応する電子メッセージポリシーについてサーバに問い合わせる動作は、ＤＮＳサーバに問い合わせる動作を含むことを特徴とする請求項８に記載の方法。
【請求項１０】
前記送信コンピュータシステムに対応する１つまたは複数の電子メッセージ送信ポリシーを受信する動作は、サーバから１つまたは複数の電子メッセージ送信ポリシー証明書を受信する動作を含むことを特徴とする請求項１に記載の方法。
【請求項１１】
前記サーバから１つまたは複数の電子メッセージ送信ポリシー証明書を受信する動作は、Ｘ．５０９証明書、ＸｒＭＬライセンス、またはＫｅｒｂｅｒｏｓ　ＰＡＣである、少なくとも電子ポリシーメッセージ証明書を受信する動作を含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記送信コンピュータシステムに対応する１つまたは複数の電子メッセージ送信ポリシーを受信する動作は、１つまたは複数のＤＮＳ　ＴＸＴレコードを受信する動作を含むことを特徴とする請求項１に記載の方法。
【請求項１３】
前記１つまたは複数のＤＮＳ　ＴＸＴレコードを受信する動作は、前記送信コンピュータシステムのサブコンピュータシステムに常駐する少なくとも１つのＤＮＳ　ＴＸＴレコードを受信する動作を含むことを特徴とする請求項１２に記載の方法。
【請求項１４】
前記送信コンピュータシステムに対応する１つまたは複数の電子メッセージ送信ポリシーを受信する動作は、前記電子メッセージ送信ポリシーをＸＭＬ命令に符号化している１つまたは複数のＤＮＳ　ＴＸＴレコードを受信する動作を含むことを特徴とする請求項１０に記載の方法。
【請求項１５】
前記電子メッセージ送信ポリシーをＸＭＬ命令に符号化している１つまたは複数のＤＮＳ　ＴＸＴレコードを受信する動作は、連結されてＸＭＬインスタンスになるように複数

のＤＮＳ　ＴＸＴレコードにわたっている電子メッセージ構成情報を受信する動作を含むことを特徴とする請求項１４に記載の方法。

【請求項１６】

前記連結されてＸＭＬインスタンスになるように複数のＤＮＳ　ＴＸＴレコードにわたっている情報を受信する動作は、複数のＤＮＳ　ＴＸＴレコード中に含まれている前記ＸＭＬ命令をどのように順序付けるべきかを示す順序付けデータを含む、前記複数のＤＮＳ　ＴＸＴレコードを受信する動作を含むことを特徴とする請求項１５に記載の方法。

【請求項１７】

前記順序付けデータに従ってＸＭＬ命令を連結することによりＸＭＬインスタンスを生成する動作をさらに含むことを特徴とする請求項１６に記載の方法。

【請求項１８】

前記１つまたは複数の受信電子メッセージ送信ポリシーから関連電子メッセージ送信ポリシーを解析する動作は、関連電子メッセージ送信ポリシーについて１つまたは複数の電子メッセージポリシー証明書を解析する動作を含むことを特徴とする請求項１に記載の方法。

【請求項１９】

１つまたは複数の送信コンピュータシステムにネットワーク接続可能な受信コンピュータシステムで使用するためのコンピュータ可読媒体であって、前記受信コンピュータシステムは前記送信コンピュータ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１つまたは複数の受信メッセージサーバを含み、前記コンピュータプ記憶媒体は、送信コンピュータシステムの電子メッセージ送信ポリシーを判断するための方法を実施し、コンピュータ実行可能命令が記憶されているコンピュータ可読媒体において、前記コンピュータ実行可能命令は、プロセッサによって実行されると、前記受信コンピュータシステムに、

前記送信コンピュータシステムから電子メッセージを受信すること、

前記送信コンピュータシステムに対応する１つまたは複数の電子メッセージ送信ポリシーを受信すること、

前記１つまたは複数の受信電子メッセージ送信ポリシーから、関連電子メッセージ送信ポリシーを解析すること、および

メッセージ分類モジュールが前記受信電子メッセージを分類する場合にさらに信頼性の高い決定を行うことが可能なように、前記関連電子メッセージ送信ポリシーを前記メッセージ分類モジュールに供給すること

を実行させることを特徴とするコンピュータ可読媒体。

【請求項２０】

１つまたは複数の送信コンピュータシステムにネットワーク接続可能な受信コンピュータシステムで使用するためのコンピュータ可読媒体であって、前記受信コンピュータシステムは前記送信コンピュータ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１つまたは複数の受信メッセージサーバを含み、前記コンピュータ記憶媒体は、メッセージ分類モジュールに供給される入力を生成するための方法を実施し、コンピュータ実行可能命令が記憶され、前記コンピュータ実行可能命令は、プロセッサによって実行されると、前記受信コンピュータシステムに、

前記送信コンピュータシステムから電子メッセージ送信ポリシーを受信すること、

前記送信コンピュータシステムに対応する電子メッセージを受信すること、

前記受信電子メッセージが不要メッセージおよび／または受信者側が送信を要求していないメッセージかどうかの判断を試みるための複数の異なるメカニズムのうち１つまたは複数を利用すること、および

メッセージ分類モジュールが前記受信電子メッセージを分類する場合にさらに信頼性の高い決定を行うことが可能なように、前記１つまたは複数の異なるメカニズムの結果のそれぞれを前記メッセージ分類モジュールに供給すること

を実行させ、

前記複数の異なるメカニズムの１つは受信した前記送信ポリシーに基づいて前記判断を

試みることを特徴とするコンピュータ可読媒体。
【請求項２１】
コンピュータ実行可能命令は、実行されると、前記受信コンピュータシステムに、前記受信電子メッセージが不要電子メッセージまたは受信者側が送信を要求していない電子メッセージかどうかの判断を試みるための複数の異なるメカニズムのうち１つまたは複数を利用させ、また、実行されると、前記受信コンピュータシステムに、電子メッセージ送信ポリシーへの遵守についてのチェックおよび送信コンピュータシステムによる努力の証拠についてのチェックを利用させるコンピュータ実行可能命令を含むことを特徴とする請求項２０に記載のコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子メール技術に関し、より詳細には、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージの低減に関する。
【背景技術】
【０００２】
コンピュータシステムおよびそれに関連する技術は、社会の多くの側面に影響を与えている。実際、コンピュータシステムの情報を処理する能力は、我々の生活の仕方、働き方を全く変えてしまった。コンピュータシステムは、今や、コンピュータシステムが出現する以前は手作業で行われていた多くの仕事（例えば、文書処理、スケジューリング、およびデータベース管理）を普通に行うようになっている。最近では、コンピュータシステムは互いに結合されて有線および無線コンピュータネットワークの両方を形成し、それらを介して電子的に通信を行うことにより）データを共用することができるようになっている。その結果、コンピュータシステムで行われる多くの　仕事（例えば、音声通信、電子メールへのアクセス、電子会議、ウェブ閲覧）は、有線および／または無線のコンピュータネットワークを介した、１つまたは複数のその他のコンピュータシステムとの電子通信を伴うようになっている。
【０００３】
不要電子メールおよび受信者側が送信を要求していない電子メール（一般に「スパム」と呼ばれている）の歴史は、事実上、電子メールの歴史と同じほど長い。これまで、スパムが与える迷惑および心配は（注目には値したが）大きな問題にはならないほど小さいものだった。しかし、最近では、ユーザの電子メールボックスにスパムが現れる割合は著しく増加してきている。大規模商用電子メールボックスプロバイダが、自分のユーザが受け取る電子メールの半分以上、さらには４分の３がスパムであることを、日常的に観察することは珍しくない。この問題は、ユーザ、産業、および経済が多大な時間と財源を当てることを強いられ、恐らく、有益な通信媒体としての電子メールの存続を危うくする恐れさえある、きわめて深刻な問題の１つとなっている。
【０００４】
従来、電子メールクライアントソフトウェアおよび電子メールサーバソフトウェアの設計は、主として、ユーザが電子メールをできるだけ効率的、有益、かつ心地よいものとして扱えるようにすることに焦点が当てられてきた。これらのソフトウェアは、送られてきた電子メールメッセージに対してユーザが実際に持つ興味については、考慮していたとしてもわずかしか考慮していない。したがって、受信された電子メールメッセージはすべて同等に扱われがちであり、それらの電子メールメッセージの内容に関係なく、ユーザに対して同じように提示されている。残念なことに、電子メールメッセージがこのように扱われていることにより、実質的に正当な電子メールメッセージ（例えば、知人である送信者からの電子メッセージ、ユーザからの送信された電子メールに対する応答）の提示と区別がつけられずにスパムが提示されている。
【０００５】
したがって、電子メールメッセージをスパムとして分類し、それによってスパムをその

他の正当な電子メールメッセージと区別するための技術がいくつか開発されている。いくつかの技術では、受信した電子メールメッセージを調べ、その中に見出される単語やフレーズに基づいて、受信した電子メールメッセージをスパムとして分類する。スパムを分類するための別の技術では、スパムである電子メールメッセージは一般に多数のユーザに送信されることを利用している。これら別の技術は、電子メールメッセージをスパムとして識別するのに一括ボーティングアプローチを使用している。別の一般的で特に有益な技術は、知人である文通相手のリストのメンテナンスをユーザに代わって行う技術であり、これは一般に「知人送信者リスト」または「ホワイトリスト」と呼ばれているアプローチである。

【０００６】

スパムとして分類した後、例えば、そのスパム電子メールメッセージを自動的にユーザの「スパムフォルダ」に移動させることにより、あるいは、可能には、ユーザがそのスパム電子メールメッセージが送られてきたことさえ知らないうちに削除することにより、スパム電子メールメッセージを正当な電子メールメッセージとは異なって扱うことができる。

【０００７】

しかし、多くの従来の電子メール分類技術は、電子メールメッセージが正当なメッセージかまたはスパムかを判断する場合に、電子メールメッセージの内容（例えば、電子メールメッセージのヘッダおよび／または本文）のみを利用している。これは問題がある。なぜならば、スパムを送りつけようとしているエンティティは、正当な電子メールメッセージに見えるように、意図的にスパム電子メールメッセージを変更できる（しかもしばしばきわめて容易に）からである。例えば、スパムを送りつけようとしているエンティティは、電子メールフィルタによって検出される可能性が低くなるように電子メールメッセージの本文を構成することができる。さらに、スパムを送りつけようとしているエンティティは、電子メールメッセージのヘッダ部分中の特定のアドレス指定情報を変更することができる。これは一般に「ドメインのなりすまし」と呼ばれている。

【０００８】

ドメイン名のなりすましには、送信者の電子メールアドレスのドメイン名（すなわち、電子メールアドレスの“＠”以降のテキスト）を変更して、その電子メールメッセージが、実際にはそれを送っていない特定のエンティティから送られれてきたかのように見せることが含まれる。この場合、電子メール分類技術は、実際にはスパムとして分類しなければならない場合に、そのなりすましのドメイン名に基づいて、電子メールメッセージを正当なメッセージとして誤って分類する場合がある。したがって、従来のメール分類技術の有効性は低減される。

【０００９】

一般に、電子メールメッセージが送信メールサーバから受信メールサーバに転送される前に、それらの送信および受信メールサーバの間に、例えば送信制御プロトコル（“ＴＣＰ”）接続などの接続が確立される。接続の確立には、ネットワークアドレス、ポート番号、および連番を含む構成情報の交換が含まれ得る。例えば、ＴＣＰ接続の確立は、周知の３方向ハンドシェイクを含む。残念なことに、ＴＣＰの３方向ハンドシェイクはよく知られているため、スパムを送りつけようとしているエンティティは、ネットワークアドレスを偽造し、次いでその偽造したネットワークアドレスから発信されたとみなされる構成情報（例えば連番）を送信することができる。受信メッセージサーバは、その構成情報が偽造ネットワークアドレスから発信されたと誤って判断する場合がある。

【発明の開示】

【発明が解決しようとする課題】

【００１０】

このように、エンティティは、ネットワークアドレスを偽造し、受信メッセージサーバにはその偽造ネットワークアドレスから発信されたように見える接続を確立することができる。したがって、このエンティティは、次いで、確立された接続を使って、その偽造ネ

ットワークアドレスから発信されたように見える電子メールメッセージを送信することができる。その後、エンティティがその偽造ネットワークアドレスのドメイン名にもなりすました場合、電子メールメッセージの真の発信ネットワークアドレスを判断することは、不可能ではないまでも難しいことがある。受信メッセージサーバは、偽造ネットワークアドレスとなりすましのドメイン名に基づいて、その電子メールメッセージを正当なメッセージとして誤って分類する場合がある。したがって、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージを調整により低減するためのメカニズムがあれば有利であろう。

【課題を解決するための手段】

【００１１】

従来技術の上述の問題点は、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージの低減のための方法、システム、コンピュータプログラム製品（コンピュータ可読媒体）、およびデータ構造を対象とした、本発明の原理によって克服される。所望の機能に応じて、複数の異なる生成入力のうち１つまたは複数を、可能には電子メッセージ中に含まれるメッセージデータとともに、メッセージ分類モジュールに供給することができる。メッセージ分類モジュールは、受信した入力に基づいて、電子メッセージを正当なメッセージ、または不要メッセージおよび受信者側が送信を要求していないメッセージとして分類することができる。複数の入力（それぞれの入力が電子メッセージの送信に関連する異なる情報を表す）を利用した場合、メッセージ分類モジュールは、電子メッセージを不要メッセージおよび／または受信者側が送信を要求していないメッセージとしてより信頼性高く分類するなど、電子メッセージをより信頼性高く分類することができる。

【００１２】

一実施形態では、標準的な接続確立データの交換が変更されて、エンティティが偽造ネットワークアドレス（例えば、偽造インターネットプロトコル（“ＩＰ”）アドレス）から電子メッセージを送信する可能性が低減される。送信側コンピュータシステムは、送信ネットワークアドレスとみなされるアドレスを含む接続開始データ（例えば、ポート、連番など）を送信する。受信側コンピュータシステムは、その送信アドレスとみなされるアドレスを含む接続開始データを受信する。受信側コンピュータシステムは、アドレス検証データを含むように標準接続確立データを変更する。受信コンピュータは、変更された接続確立データを送信ネットワークアドレスとみなされるアドレスに送信する。

【００１３】

送信ネットワークアドレスとみなされるアドレスが送信コンピュータシステムに対応する場合、送信コンピュータシステムは、アドレス検証データを含む変更済み接続確立データを受信することができる。したがって、送信側コンピュータシステムは、そのアドレス検証データに基づいて、適切な接続応答データを生成することができる。一方、送信ネットワークアドレスとみなされるアドレスが送信コンピュータシステムに対応しない場合（例えば、ネットワークアドレスが偽造されている場合）、送信コンピュータシステムは、アドレス検証データを含む変更済み接続確立データを受信しない。

【００１４】

送信側コンピュータシステムが受信コンピュータシステムに標準接続応答データを送信する場合がある（例えば、送信アドレスとみなされるアドレスに対応しないコンピュータシステムから、標準接続応答データのシミュレーションを試みようとする場合）。しかし、送信側コンピュータシステムはアドレス検証データを知らないため、アドレス検証データに適切に応答することができない。受信側コンピュータシステムは、送信ネットワークアドレスとみなされるアドレスに対応するコンピュータシステムがアドレス検証データ適切に応答したかどうかを判断する。

【００１５】

別の実施形態では、あるドメイン（例えば、“ｔｅｓｔ．ｃｏｍ”）のネームサービス（例えば、ドメインネームサービス）エントリが、そのドメインへの送信メッセージを扱

うことを許可されているコンピュータシステムのネットワークアドレス（例えばＩＰアドレス）を含むように構成される。すなわち、ネームサーバエントリが、そのドメインのために電子メッセージを送信することを許可されているコンピュータシステムのネットワークアドレスで構成される。受信メッセージサーバは、送信側ドメインから送信されたとみなされる電子メッセージを受信する。受信メッセージサーバは、その電子メッセージを送った送信メッセージサーバに対応する実際の送信側ネットワークアドレスを識別する（例えば、接続確立データから）。

【００１６】

受信メッセージサーバは、その送信ドメインのために電子メッセージを送信することを許可されたネットワークアドレスのリストを、ネームサーバに問い合わせる。受信メッセージサーバは、実際の送信側ネットワークアドレスが許可ネットワークアドレスリストに含まれているかどうかを判断する。受信メッセージサーバは、判断の結果（すなわち、送信コンピュータシステムがドメインのために電子メッセージを送信することを許可されているか、または許可されていないか）をメッセージ分類モジュールに供給する。

【００１７】

さらに別の実施形態では、電子メッセージ送信ポリシー（“ＥＴＰ”）が、ドメインのネームサービスエントリ中に、または受信電子メッセージ中に含まれている。ＥＴＰ証明書を使って、送信ドメインが遵守しているＥＴＰを受信コンピュータシステムに示すことができる。受信メッセージサーバは、送信ドメインから電子メッセージを受信する。受信メッセージサーバは、送信ドメインに対応する１つまたは複数のＥＴＰ（例えば、ＥＴＰ証明書に含まれているＥＴＰ）を受信する。受信メッセージサーバは、例えば、ネームサーバに問い合わせることにより、あるいは受信電子メッセージからＥＴＰを抽出することにより、ＥＴＰを受け取ることができる。

【００１８】

受信メッセージサーバは、関連するＥＴＰを解析する。関連ＥＴＰは、送信ドメインが遵守しているＥＴＰを示す。受信メッセージサーバは、その関連ＥＴＰをメッセージ分類モジュールに供給する。

【００１９】

さらに別の実施形態では、送信コンピュータシステムは、電子メッセージを送信する前に計算リソースが消費されたことを受信コンピュータシステムに示す。送信コンピュータシステムが計算パズルに適切な解決を与えた場合、消費された計算リソースを、受信コンピュータシステムが少なくとも見積もることができる。計算パズルは、適切な解決（例えば、強引なアプローチを使って識別される解決）を生成するために、送信コンピュータシステムがより多くの計算リソースを消費することを要求されるように構成することができる。しかし、受信コンピュータシステムにおいては、適切な解決を確認するのに著しく低減された計算リソースしか消費されない。確認可能な解決を計算することは、基本的に、電子メッセージ送信者が、電子メッセージを電子メッセージ受信側に送信するためのチケットを購入する（消費されたプロセッササイクルを通して）ことになる。このような計算パズルの１つは、応答ドキュメントの強引な計算を行うものである。

【００２０】

送信メッセージサーバは、電子メッセージに含めるべき電子メッセージデータを受信する。送信メッセージサーバは、例えば、その電子メッセージデータおよび／またはその他の状態情報の異なる部分から、初期ドキュメントを生成する。パズル入力は、電子メッセージの１つまたは複数の構成要素から生成される。パズル入力は、特に不要メッセージおよび／または受信者側が送信を要求していないメッセージを阻止する際に使用するように設計された、パズルハッシュアルゴリズムに供給される。例えば、パズルハッシュアルゴリズムは、ＳＨＡ－１アルゴリズムのハッシュ副関数を利用し得るが、それらの副関数を、ＳＨＡ－１アルゴリズムとは異なる順序で適用する。副関数を異なる順序で適用することによって、パズルハッシュアルゴリズムをハードウェアに実装することがより困難になり、また、正当な必要性のためにハッシュアルゴリズムのハードウェア加速が望まれる問

題空間とは区別されて使用される。

【００２１】

実施形態によっては、パズル入力が初期ドキュメントである。別の実施形態では、初期ドキュメントおよびその他のメールメッセージデータからパズル入力が計算される。

【００２２】

送信メッセージサーバは、応答ドキュメントとパズル入力（初期ドキュメントまたはパズル入力ハッシュ値のいずれか）との結合から計算された（パズルハッシュアルゴリズムを使って）応答ハッシュ値が計算パズルの応答値になるように、応答ドキュメントを識別する。例えば、応答ドキュメントを使って、先頭に指定数のゼロを有する応答ハッシュ値を計算することができる。送信メッセージサーバは、メッセージデータと応答ドキュメントを含む電子メッセージを受信ドメインに送信する。

【００２３】

受信ドメインの受信コンピュータシステムがこの電子メッセージを受信する。受信コンピュータシステムは、例えば、送信コンピュータシステムで使用されたメッセージおよび／またはその他の状態情報の異なる部分から、初期ドキュメントを再生する。受信コンピュータシステムは、初期ドキュメントからパズル入力を再計算する（可能には、パズルハッシュアルゴリズムを使ってパズル入力ハッシュ値を計算する）。受信コンピュータシステムは、応答ドキュメントとパズル入力（初期ドキュメントかパズル入力ハッシュ値のいずれか）との結合から計算された（パズルハッシュアルゴリズムを使って）確認ハッシュ値が、計算パズルの解決を示す応答であるかどうか（例えば、確認ハッシュ値が先頭に指定数のゼロを有するかどうか）を判断する。受信コンピュータシステムは、判断の結果（例えば、送信メッセージサーバが確認可能または確認不可能な解決を供給した、あるいは何も解決を供給しなかったなど）をメッセージ分類モジュールに供給する。

【００２４】

本発明のさらなる特徴および利点を、以下に説明する。それらの一部はその説明から明らかになるであろうし、あるいは、本発明を実施することによりわかる場合もあろう。本発明の特徴および利点は、特に添付の特許請求の範囲において指摘している機器および組合せを用いることにより実現することができ、また得ることができる。本発明のこれらおよびその他の特徴は、以下の説明および添付の特許請求の範囲からより十分に明らかになるであろう。あるいは、以下の説明のように本発明を実施することによってわかる場合もあろう。

【００２５】

本発明の上述およびその他の利点および特徴を得ることが可能な方法を説明するために、上記に簡単に説明した本発明を、添付の図面に図示したそれらの具体的な実施形態を参照しながらより詳細に説明する。それらの図面が本発明の代表的な実施形態を表したものにすぎず、したがって本発明の範囲を限定するものとしてみなすべきものではないことを理解した上で、本発明を、添付の図面を使用しながら、さらなる特性および詳細を示して説明する。

【発明を実施するための最良の形態】

【００２６】

本発明の原理は、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージを調整により低減するための方法、システム、コンピュータプログラム製品、およびデータ構造を対象としている。接続確立データの交換が変更されることにより、エンティティが偽造ネットワークアドレスを含む電子メッセージを送るリスクを低減し、また防げる可能性がある。受信メッセージサーバは、許可送信サーバリストをチェックして、あるドメインのために電子メッセージを送信することが認可されているサーバを識別する。送信メッセージサーバは、ドメインの電子メッセージ送信ポリシーを識別する。送信メッセージサーバは、計算パズルに対する応答を計算し、受信メッセージサーバは、それを確認する。送信サーバリストのチェック、識別された電子メッセージ送信ポリシー、およびパズル応答確認を、その他の入力と共に電子メッセージ分類モジュールに供給することが

できる。

【００２７】

本発明の範囲に含まれる実施形態には、コンピュータ実行可能命令またはデータ構造を運ぶ、あるいは保持しているコンピュータ可読媒体が含まれる。このようなコンピュータ可読媒体は、汎用または専用コンピュータシステムがアクセス可能ないずれかの入手可能な媒体であってよい。例として、このようなコンピュータ可読媒体には、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭ、ＣＤ－ＲＯＭまたはその他の光ディスク記憶装置、あるいは磁気ディスクストレージまたはその他の磁気記憶装置などの物理記憶媒体、あるいは、所望のプログラムコード手段をコンピュータ実行可能命令、コンピュータ可読命令、またはデータ構造の形態で運ぶ、または記憶するために使用することができ、また、汎用または専用コンピュータシステムがアクセス可能ないずれかのその他の媒体が含まれるが、それらに限定されるわけではない。

【００２８】

情報がネットワークまたはその他の通信接続（有線、無線、または有線と無線の組合せのうちいずれか）を介してコンピュータシステムに転送または提供される場合、その接続はコンピュータ可読媒体として正しくみなされる。したがって、いずれかのこのような接続も、コンピュータ可読媒体と正しく呼ばれる。上記を組み合わせたものも、コンピュータ可読媒体の範囲に含まれるものとする。コンピュータ実行可能命令またはコンピュータ可読命令には、例えば、汎用コンピュータシステムまたは専用コンピュータシステムに特定の機能または機能グループを実行させる命令またはデータが含まれる。コンピュータ実行可能またはコンピュータ可読命令とは、例えば、バイナリ、アセンブリ言語などの中間書式命令、さらにはソースコードの場合がある。

【００２９】

この説明および添付の特許請求の範囲では、「コンピュータシステム」を、協働して電子データ上で動作する、１つまたは複数のソフトウェアモジュール、１つまたは複数のハードウェアモジュール、またはそれらの組合せとして定義している。例えば、コンピュータシステムの定義には、パーソナルコンピュータのハードウェアモジュール、およびパーソナルコンピュータのオペレーティングシステムなどのソフトウェアモジュールが含まれる。モジュールの物理的なレイアウトは重要ではない。コンピュータシステムは、ネットワークを介して結合された１つまたは複数のコンピュータを含む場合がある。同様に、コンピュータシステムは、内部モジュール（プロセッサおよびメモリなど）が協働して電子データ上で動作する、単一の物理デバイス（携帯電話またはパーソナルディジタルアシスタント“ＰＤＡ”など）を含む場合がある。

【００３０】

当業者は、本発明を、ハブ、ルータ、無線アクセスポイント（“ＡＰ”）、無線局、パーソナルコンピュータ、ラップトップコンピュータ、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースの、またはプログラム可能な家庭用電子機器、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、携帯電話、ＰＤＡ、ページャなどを含む、様々なタイプのコンピュータシステム構成を備えたネットワークコンピューティング環境において実施できることを理解されよう。本発明はまた、ネットワークを介してリンクされた（無線、有線、または有線接続と無線接続の組合せのいずれかによって）ローカルおよびリモートのコンピュータシステムが共にタスクを実行する、分散システム環境においても実施することができる。

【００３１】

図１は、本発明の原理に従って接続ハイジャックの低減を実施する、ネットワークアーキテクチャ１００の一例を示している。ネットワークアーキテクチャ１００内では、送信メッセージサーバ１０７、受信メッセージサーバ１０９、およびメッセージサーバ１８４が、それぞれ、対応するリンク１０２、１０４、および１０３によってネットワーク１０１に接続されている。同様に、ネームサーバ１０８が、リンク１０６によってネットワーク１０１に接続されている。リンク１０２、１０３、１０４および１０６、およびネット

ワーク１０１は、システムバスの一部、ローカルエリアネットワーク（“ＬＡＮ”）の一部、広域ネットワーク（“ＷＡＮ”）の一部、および／またはインターネットの一部さえも含み得る。両方向矢印１８６が示すように、ネームサーバ１０８は、反復クエリの目的で、その他のネームサーバ１８５と通信することもできる。同様に、ネットワークアーキテクチャ１００内のコンピュータシステムは、反復クエリの目的で、その他のネームサーバ１８５に直接、問い合わせることができる（ただし、ネットワークアーキテクチャ１００内のコンピュータシステムをその他のネームサーバ１８５に接続するリンクは明示していない）。

【００３２】

メッセージクライアント１３２および１３３は、それぞれ、対応するリンク１３６および１３７によって、受信メッセージサーバ１０９に接続されている。メッセージエンティティ（例えば、ユーザまたは法人）は、メッセージクライアント１３２および１３３を利用して、受信メッセージサーバ１０９に記憶されている電子メッセージにアクセスすることができる。

【００３３】

送信メッセージサーバ１０７、受信メッセージサーバ１０９、およびメッセージサーバ１８４は、送信制御プロトコル（“ＴＣＰ”）を利用して、相互間の接続、およびその他のコンピュータシステムとの接続を確立する電子メッセージサーバであり得る。送信メッセージサーバ１０７、受信メッセージサーバ１０９、およびメッセージサーバ１８４はまた、簡易メール転送プロトコル（“ＳＭＴＰ”）を利用して、その他のメッセージサーバおよびその他のコンピュータシステムと電子メールメッセージを交換することができる（例えば、確立されたＴＣＰ接続を介して）。ネームサーバ１０８は、ドメイン名（例えば、ｗｗｗ．ｔｅｓｔ．ｃｏｍ）をインターネットプロトコル（“ＩＰ”）アドレス（例えば、１１２．４５．１２３．９９）に変換する、ドメインネームシステム（“ＤＮＳ”）サーバであり得る。

【００３４】

ネームサーバ１０８は、あるドメインが、例えば拡張ＮＯＯＰコマンドに対するサポートやその他のＳＭＴＰ拡張コマンドに対するサポートなど、非標準接続確立データの交換をサポートしていることを表す１つまたは複数のレコードを記憶することができる。非標準接続確立データの交換に対するサポートを表すレコードは、例えば特別なＮＯＯＰレコード、ＴＸＴレコード、または１組のＴＸＴレコードなどのＤＮＳレコードであり得る。ＴＸＴレコードまたは１組のＴＸＴレコードは、テキストデータ、または、例えば拡張マークアップ言語（“ＸＭＬ”）命令など、テキストフォームで符号化されたその他のデータを含むことができる。非標準接続確立データの交換に対するサポートを表すレコードは、ドメインの電子メールポリシーを表すＤＮＳレコードセットに含むことができる。

【００３５】

図２は、本発明の原理に従って接続ハイジャックを低減するための方法２００の例示的流れ図を示す。方法２００を、ネットワークアーキテクチャ１００中に示す構成要素に関して説明する。方法２００は、送信アドレスとみなされるアドレスを含む接続開始データを受信コンピュータシステムに送信する動作を含む（動作２０１）。動作２０１は、送信コンピュータシステムが送信接続開始データを受信コンピュータシステムに送る動作を含むことができる。接続開始データは、例えば、送信メッセージサーバと他のコンピュータシステムの間のＴＣＰまたはＳＭＴＰ接続などの、接続の確立を開始するためのデータであり得る。したがって、接続開始データは、接続確立を開始するための連番、ポート番号、またはその他の適切なコマンドも含み得る。

【００３６】

例えば、送信メッセージサーバ１０７は、アドレス１１２を含む接続開始データ１１１を受信メッセージサーバ１０９に送ることができる。これは、送信メッセージサーバ１０７が、メッセージサーバ１８４に対応するネットワークアドレス（例えば、ＩＰアドレス）のハイジャックを試みている場合があり得る。この場合、アドレス１１２は、メッセー

ジサーバ１８４に対応するネットワークアドレスであり得る。一方、送信メッセージサーバ１０７がネットワークアドレスのハイジャックを試みているのではなく、アドレス１１２が送信メッセージサーバ１０７に対応するネットワークアドレスの場合もあり得る。接続開始データ１１１は、例えば、送信メッセージサーバ１０７が送信するＳＭＴＰ　ＨＥＬＯコマンドまたはＳＭＴＰ　ＥＨＬＯコマンドに含めることができる。

【００３７】

方法２００は、送信アドレスとみなされるアドレスを含む接続開始データを、送信コンピュータシステムから受信する動作（動作２０５）を含む。動作２０５は、受信コンピュータシステムが送信コンピュータシステムから接続開始データを受信する動作を含むことができる。受信した接続開始データは、例えば、受信メッセージサーバと他のコンピュータシステムとの間のＴＣＰまたはＳＭＴＰ接続などの、接続の確立を開始するためのデータであり得る。例えば、受信メッセージサーバ１０９は、アドレス１１２を含む接続開始データ１１１を送信メッセージサーバ１０７から受信することができる。接続開始データ１１１は、受信メッセージサーバ１０９において受信されるＳＭＴＰ　ＨＥＬＯコマンドに含めることができる。

【００３８】

方法２００は、アドレス検証データを含むように標準接続確立データを変更する動作（動作２０６）を含む。動作２０６は、受信コンピュータシステムがアドレス検証データを含むように標準接続確立データを変更する動作を含むことができる。例えば、受信メッセージサーバ１０９は、本来ならば接続開始データ１１１に応答してアドレス１１２に送信されるはずの標準接続確立データを変更することができる。接続開始データ１１１がＴＣＰ接続を確立すべきであることを表している場合、受信メッセージサーバ１０９は、標準接続応答データを複数のネットワークパケットに分解する。あるいは、接続開始データ１１１がＴＣＰ接続を確立すべきであることを表している場合、受信メッセージサーバ１０９は、接続開始データ１１１を削除することができる。実施形態によっては、接続開始データ１１１を受信したことに応答して、受信メッセージサーバ１０９が、ランダムな文字列（またはその他の非標準データの一部）を含むように標準接続確立データを変更する。

【００３９】

方法２００は、変更した接続確立データを送信アドレスとみなされるアドレスに送信する動作（動作２０７）を含む。動作２０７は、受信コンピュータシステムが、変更した接続確立データを送信アドレスとみなされるアドレスに送信する動作を含むことができる。例えば、アドレス１１２が送信メッセージサーバ１０７に対応する場合、受信メッセージサーバ１０９は、アドレス検証データ１１４を含む変更済み接続確立データ１１３を送信メッセージサーバ１０７に送信することができる。一方、アドレス１１２がメッセージサーバ１８４に対応する場合は、受信メッセージサーバ１０９は、アドレス検証データ１１４を含む変更済み接続確立データ１１８をメッセージサーバ１８４に送ることができる。

【００４０】

変更済み接続確立データ１１３および１１８は、接続確立データを含む連続したパケットの最後のネットワークパケット、接続開始データの再送信要求、あるいはランダムな文字列（またはその他の非標準データの部分）を含むＳＭＴＰ　ＨＥＬＯ応答またはＳＭＴＰ　ＥＨＬＯ応答コマンドであり得る。これらのタイプの接続確立データは標準接続確立データとは異なる。したがって、ネットワークアドレスのハイジャックしようとしているコンピュータシステムがこの変更された接続確立データに対する適切な応答を正しく予測できる可能性は低くなる。

【００４１】

方法２００は、アドレス検証データを含む変更済み接続確立データを受信する動作（動作２０２）を含む。動作２０２は、送信コンピュータシステムが、アドレス検証データを含む変更済み接続確立データを受信する動作を含むことができる。例えば、送信メッセージサーバ１０７は、アドレス検証データ１１４を含む変更済み接続確立データ１１３を受信メッセージサーバ１０９から受信することができる。

【００４２】
実施形態によっては、接続開始データを送信していないメッセージサーバが変更済み接続確立データを受け取る。例えば、アドレス１１２がメッセージサーバ１８４に対応する場合、メッセージサーバ１８４は、アドレス検証データ１１４を含む変更済み接続確立データ１１８を受信メッセージサーバ１０９から受信することができる。受信された変更済み接続確立データ１１８が対応する接続開始データに応答して受信されたのではない場合、メッセージサーバ１８４は、単に変更済み接続確立データ１１８を廃棄する。したがって、送信メッセージサーバ１０７がメッセージサーバ１８４からの接続のシミュレーション（およびそれによるハイジャック）を試みている場合、受信メッセージサーバ１０９は、アドレス検証データ１１４に対する適切な応答を受信することができない。例えば、受信メッセージサーバ１０９は、アドレス検証データ１１４中に含まれているランダムな文字列をエコーバックする拡張ＮＯＯＰコマンドを受信することができない。

【００４３】
したがって、受信メッセージサーバ１０９は、ネームサーバ１０８に問い合わせて、メッセージサーバ１８４（アドレス１１２に対応するメッセージサーバ）が変更済み接続確立データをサポートしているかどうかを判断することができる。エントリ１７６は、メッセージサーバ１８４を含むドメインのＤＮＳエントリであり得る。受信メッセージサーバ１０９は、変更済み接続確立サポートレコード、例えば拡張ＮＯＯＰサポートレコード１３８（特別なＮＯＯＰサポートレコードまたはＴＸＴレコード）について、エントリ１７６に問い合わせることができる。メッセージサーバ１８４が変更済み接続確立、例えば拡張ＮＯＯＰコマンドをサポートすることが示される場合、アドレス検証データ１１４への適切な応答を受信できないことは、接続開始データ１１１がメッセージサーバ１８４から送信されていないことを表しているはずである。

【００４４】
方法２００は、アドレス検証データに基づいて適切な接続応答データを生成する動作（動作２０３）を含む。動作２０３は、送信コンピュータシステムが、アドレス検証データに基づいて適切な接続応答データを生成する動作を含むことができる。例えば、送信メッセージサーバ１０７は、アドレス検証データ１１４に基づいて適切な接続応答データ１１７を生成することができる。接続確立データ１１３が複数のネットワークパケットにおける最後のネットワークパケットである場合、送信メッセージサーバ１０７は、その最後のネットワークパケットに該当する連番確認メッセージを生成することができる。接続確立データ１１３が接続開始データ１１１の再送信要求である場合、送信メッセージサーバ１０７は接続開始データ１１１を再生成することができる。接続確立データが非標準データ（例えば、ランダムな文字列）を含むＳＭＴＰ　ＨＥＬＯ応答コマンドまたはＳＭＴＰ　ＥＨＬＯ応答コマンドである場合、送信メッセージサーバ１０７は、その非標準データを含む拡張ＮＯＯＰコマンドを生成することができる。

【００４５】
方法２００は、適切な接続応答データを受信コンピュータシステムに送信する動作（動作２０４）を含む。動作２０４は、送信コンピュータシステムが適切な接続応答データを受信コンピュータシステムに送信する動作を含むことができる。例えば、送信メッセージサーバ１０７は、適切な接続応答データ１１７を含む接続応答データ１１６を、受信メッセージサーバ１０９に送信することができる。適切な接続応答データ１１７は、例えば、該当する確認連番、再生成された接続開始データ、または非標準データを含むことができる。送信メッセージサーバ１０７が、例えば受信したＳＭＴＰ　ＨＥＬＯコマンドまたはＳＭＴＰ　ＥＨＬＯコマンドからのランダムな文字列を拡張ＮＯＯＰコマンドに含める場合がある。

【００４６】
受信メッセージサーバ１０９は、接続応答データ１１６を受信することができる。しかし、受信メッセージサーバは、適切な接続応答を含んでいないその他の接続応答データを受信したり、あるいは接続応答データを全く受信しない場合もある。例えば、送信メッセ

ージサーバ１０７がメッセージサーバ１８４に対応するネットワークアドレスをハイジャックしようとしている場合、送信メッセージサーバ１０７はアドレス検証データ１１４を受信しない場合がある（アドレス検証データ１１４がメッセージサーバ１８４に送信されないために）。したがって、送信メッセージサーバ１０７は、アドレス検証データ１１４に基づかない接続応答データを予測しようとする。したがって、送信メッセージサーバ１０７が不適切な（例えば、標準の）接続応答データを予測する可能性が高くなる。

【００４７】

方法２００は、送信アドレスとみなされるアドレスに対応するコンピュータシステムが、アドレス検証データに適切に応答したかどうかを判断する動作（動作２０８）を含む。動作２０８は、受信コンピュータシステムが、送信アドレスとみなされるアドレスに対応するコンピュータシステムがアドレス検証データに適切に応答したかどうかを判断する動作を含むことことができる。例えば、受信メッセージサーバ１０９は、アドレス１１２に対応するコンピュータシステムがアドレス検証データ１１４に適切に応答したかどうかを判断することができる。適切な接続応答データ１１７を受信することによって、受信メッセージサーバ１０９は、アドレス１１２に対応するコンピュータシステムが適切に１１４に応答したことを知ることができる。例えば、接続確立データ１１３を含むネットワークパケットに該当する確認連番、再送信要求に応答しての接続開始データ１１１の再送信、またはランダムなエコー文字列を含む拡張ＳＭＴＰ　ＮＯＯＰコマンドが適切な接続応答を表すことができる。受信メッセージサーバ１０９が適切な接続応答を受信した場合、ネットワークアドレスとみなされるアドレスがハイジャックされている可能性は低い。

【００４８】

不適切な接続データに応答して、受信メッセージサーバは、送信アドレスとみなされるアドレスに対応するネームサーバエントリに問い合わせることができる。例えば、受信メッセージサーバ１０９はエントリ１７６（アドレス１１２に対応するエントリ）に問い合わせて、メッセージサーバ１８４が変更済み接続確立をサポートしているかどうかを判断することができる。メッセージサーバ１８４が変更済み接続確立データ、例えば拡張ＮＯＯＰコマンドをサポートしていることが示された場合、メッセージサーバ１８４からのものとみなされる不適切な応答データの受信は、接続開始データ１１１がメッセージサーバ１８４から送信されたものではないことを表すはずである。

【００４９】

次に図３を参照すると、図３は、本発明に従って許可された送信メッセージサーバの識別を実施する、ネットワークアーキテクチャ３００の一例を示している。ネットワークアーキテクチャ３００には、ドメイン３０５、３０６、および３０７を示してある。ドメイン３０５、３０６、および３０７を、それらがそれらの内に示されている対応コンピュータシステムを論理的に含んでいることを説明するために、破線で示してある。しかし、あるドメインに含まれるコンピュータシステムの物理的な場所は互いに異なってよい。例えば、メッセージクライアント３４１およびメッセージクライアント３４３は、物理的にきわめて近くに（例えば、同じ部屋に）位置することも可能であるし、あるいは、物理的にきわめて離れて（例えば、異なる大陸に）位置することも可能である。

【００５０】

ネットワークアーキテクチャ３００にはネームサーバ３０８も示してある。一般に、ネームサーバ３０８は、例えば、異なるドメインにあるコンピュータシステム間の通信を実施するために、コンピュータシステムのテキスト列識別子を対応する数値のネットワークアドレスに対応付けるネーム情報を記憶している。ネームサーバ３０８は、ドメイン名（例えば、ＷＷＷ．ｔｅｓｔ．ｃｏｍ）をインターネットプロトコル（“ＩＰ”）アドレス（例えば、１０２．３３．２３．１１２）に変換するドメインネームシステム（“ＤＮＳ”）サーバの場合がある。

【００５１】

ネームサーバ１０８は、あるドメインのための許可された送信メッセージサーバを表す１つまたは複数のレコードを記憶することができる。ドメインのための許可された送信メ

ッセージサーバを表すレコードは、例えば、ＲＭＸレコード、ＴＸＴレコード、または１組のＴＸＴレコードなどのＤＮＳレコードであり得る。ＴＸＴレコードまたは１組のＴＸＴレコードは、テキストデータ、または、例えばＸＭＬ命令など、テキストフォームで符号化されたその他のデータを含むことができる。許可された送信メッセージサーバを示すレコードは、ドメインの電子メールポリシーを示すＤＮＳレコードセット中に含めることができる。

【００５２】

ネットワークアーキテクチャ３００にはネットワーク３０１も示してある。ドメイン３０５、ドメイン３０６、ドメイン３０７、およびネームサーバ３０８は、それぞれ、対応するリンク３９１、３９２、３９３、および３９４によってネットワーク３０１に接続されている。リンク３９１、３９２、３９３および３９４、およびネットワーク３０１は、システムバスの一部、ローカルエリアネットワーク（“ＬＡＮ”）の一部、広域ネットワーク（“ＷＡＮ”）の一部、および／またはインターネットの一部さえも含むことができる。ネットワークアーキテクチャ３００内に示してあるドメインおよびコンピュータシステムは、図示のリンクを介して、例えば、電子メールメッセージ、ＤＮＳクエリ、ＤＮＳ応答（リソースレコードを含む）などの電子メッセージを交換することができる。両方向矢印３８６で示すように、ネームサーバ３０８は、反復クエリの目的でその他のネームサーバ３８５と通信することもできる。同様に、ネットワークアーキテクチャ３００内のコンピュータシステムは、反復クエリの目的で、その他のネームサーバ３８５に直接、問い合わせることができる（ただし、ネットワークアーキテクチャ３００内のコンピュータシステムをその他のネームサーバ３８５に接続するリンクは明示していない）。

【００５３】

ドメイン３０７内において、メッセージクライアント３４１および３４３は、それぞれ、対応するリンク３９６および３９７によってメッセージサーバ３１７に接続されている。メッセージクライアント３４１および３４３はそれぞれ、例えば電子メールクライアントソフトウェアに含まれた、対応するメッセージインタフェースモジュール（図示せず）を含むことができる。メッセージインタフェースモジュールは、メッセージクライアントの１つのユーザに、メッセージサーバ３１７にアクセスして電子メッセージを見るためのメカニズムを提供する。ユーザ（例えば、Ｊｏｈｎ　Ｄｏｅ）は、このユーザに割り当てられ、かつ／またはこのユーザによる使用が許可されている電子メッセージアドレス（例えば、ｊｄｏｅ@ｔｅｓｔ２．ｃｏｍ）に送信された電子メッセージを見ることができる。

【００５４】

図４は、本発明に従って許可された送信メッセージサーバを識別するための方法４００の例示的流れ図を示す。許可されていないコンピュータシステムは、電子メッセージの１つまたは複数のフィールドを変更して（以下、これを「ドメインのなりすまし」と呼ぶ）、実際には電子メッセージ（例えば、電子メールメッセージ）がそこから送信されていない場合に、指定したドメインから送信されたように見せることができる。したがって、方法４００は、電子メッセージに含まれるドメイン名がなりすましである可能性を示す入力を供給するための方法とみることもできる。ドメイン名がなりすましである可能性が高いことは、電子メッセージが不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージであることを表す（単独で、または他の入力との組合せによって）場合がある。

【００５５】

ネットワークアーキテクチャ３００内に示してある構成要素に関して、方法４００を説明する。方法４００は、送信側ドメインから送信されたとみなされる電子メッセージを受信する動作（動作４０１）を含む。動作４０１は、受信側ドメイン中の受信メッセージサーバが、送信側ドメインから送信されたとみなされる電子メッセージを受信する動作を含むことができる。例えば、メッセージサーバ３１７（ドメイン３０７内の）は、メッセージサーバ３１６から電子メッセージ３７１を受信することができる。電子メッセージ３７

１は、電子メッセージ３７１がドメイン３０５から送信されたことを示す、なりすましドメイン名３７２を含む。

【００５６】

送信ドメインとみなされるドメインは、電子メッセージに含まれるパラメータ値から識別することができる。例えば、メッセージサーバ３１７は、電子メッセージ３７１に含まれるパラメータ値から（例えば、なりすましドメイン名３７２から）ドメイン３０５を識別することができる。送信ドメインとみなされるドメインは、送信エンティティとみなされるエンティティのドメイン部分（例えば、“＠”文字以降の文字群）から識別することができる。電子メッセージ中のその他のパラメータ値には、実際の送信ネットワークアドレスを含めることができる。例えば、実際の送信ネットワークアドレスは、電子メッセージの逆パス（差出人アドレスと呼ぶことがある）中に含まれ得る。逆パスは、送信コンピュータシステムがＳＭＴＰの“ＭＡＩＬ　ＦＲＯＭ”コマンドを発行した結果として電子メッセージに含まれ得る。したがって、メッセージサーバ３１７は、電子メッセージ３７１のこのパラメータ値を調べて、実際の送信ネットワークアドレス（例えば、メッセージサーバ３１６の実際のＩＰアドレス）の識別を試みることができる。

【００５７】

しかし、実際の送信ネットワークアドレスが、電子メッセージの第１の再送信差出人ヘッダ、電子メッセージの再送信差出人アドレスヘッダ中の第１のメールボックス、電子メールの差出人ヘッダ、または電子メッセージの差出人アドレスヘッダの第１のメールボックス中に含まれる場合もある。したがって、メッセージサーバ３１７は、電子メッセージ３７１のこれらのパラメータ値をそれぞれ調べて（別途に、あるいは逆パスパラメータ値を調べることと組み合わせて）、実際の送信ネットワークアドレス（例えば、メッセージサーバ３１６の実際のＩＰアドレス）の識別を試みることができる。電子メッセージのいくつかの異なる部分を調べるので、電子メッセージの実際の送信ネットワークアドレスを識別できる可能性が高くなる。電子メールの実装によっては、逆パスを空にして電子メッセージを送信することが要求される。本発明の実施形態は、電子メッセージが逆パスパラメータ値を含まない場合に実際の送信アドレスを識別するのに有利であり得る。

【００５８】

なりすましドメイン３７２に基づいて、メッセージサーバ３１７は、ドメイン３０５を、電子メッセージ３７１の送信ドメインとみなされるドメインとして識別する場合がある。逆パスまたはリストされたヘッダの少なくとも１つを含まない電子メッセージは、不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージとみなされる場合がある。このような電子メッセージを不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージとみなすことによって、エンティティがメッセージ分類モジュール欺くために意図的に逆パスおよび全てのヘッダを省略する可能性が低減される。

【００５９】

方法４００は、電子メッセージの複数のパラメータ値を調べて、送信コンピュータシステムに対応する実際の送信側ネットワークアドレスの識別を試みる動作（動作４０２）を含む。動作４０２は、受信側コンピュータシステムが、送信コンピュータシステムに対応する実際の送信側ネットワークアドレスを識別する動作を含むことができる。受信側コンピュータシステムは、例えば、電子メッセージ３７１の逆パス、第１の再送信差出人ヘッダ、再送信差出人アドレスヘッダ中の第１のメールボックス、電子メッセージの差出人ヘッダ、または差出人アドレスヘッダの第１のメールボックスの１つまたは複数から、実施の送信側ネットワークアドレスを識別することができる。メッセージサーバ３１７は、実際の送信側ＩＰアドレスがメッセージサーバ３１６に対応していることを識別できる。方法２００を利用して、ＩＰアドレスがなりすましである可能性を低減することができる。

【００６０】

方法４００は、ある送信側ドメインのために電子メッセージを送信することを許可されているネットワークアドレスのリストを、ネームサーバに問い合わせる動作（動作４０３

）を含む。動作４０３は、受信コンピュータシステムが、送信側ドメインのために電子メッセージを送信することを許可されているネットワークアドレスのリストを、ネームサーバに問い合わせる動作を含むことができる。例えば、メッセージサーバ３１７は、ドメイン３０７に、許可サーバクエリ３７９を含むネームサービスメッセージ３７５をネームサーバ３０８へ発行させることができる。ネームサービスメッセージ３７５は、ドメイン３０５を識別する識別子を含むことができる。

【００６１】

ネームサーバ３０８は、ネームサービスメッセージ３７５を受け取り、それに応じて許可サーバクエリ３７９を処理する。ネームサーバ３０８では、エントリ３７６がドメイン３０５に対応するＤＮＳエントリである場合がある。エントリ３７６は、許可サーバレコード３３６を含む、ドメイン３０５についての１つまたは複数のレコード（例えば、ＲＭＸおよび／またはＴＸＴレコード）を含むことができる。受信したＴＸＴレコードは、ＸＭＬ命令を含み得る。許可サーバレコード３３６はドメイン１０５のために電子メッセージを送信することを許可されたメッセージサーバに対応するネットワークアドレス（例えば、ＩＰアドレス）を含むことができる。

【００６２】

メッセージサーバ３１５がドメイン３０５からの電子メッセージを送信することを許可されたコンピュータシステムとして指定され、しかし、メッセージサーバ３１６が３０５からの電子メッセージを送信することを許可されたコンピュータシステムとして指定されていない場合がある。この場合、許可サーバレコード３３６を、メッセージサーバ３１５に対応するメッセージアドレス（および、可能には、その他のコンピュータシステムのネットワークアドレス）を含むように、しかしメッセージサーバ３１６に対応するネットワークアドレスを含まないように構成することができる。したがって、ネームサービスメッセージ３７５を受信したことに応答して、ネームサーバ３０８は、許可サーバリスト３７８を含むネームサーバ応答３７７をドメイン３０７に送信することができる。ドメイン３０７は、ネームサーバ応答３７７を受信し、それをメッセージサーバ３１７に転送することができる。

【００６３】

方法４００は、実際の送信側ネットワークアドレスが送信ドメインのために送信電子メッセージを送信することを許可されているかどうかを判断する動作（動作４０４）を含む。動作４０４は、受信コンピュータシステムが、実際の送信側ネットワークアドレスが送信ドメインのために送信電子メッセージを送信することを許可されているかどうかを判断する動作を含むことができる。例えば、メッセージサーバ３１７は、メッセージサーバ３１６に対応するネットワークアドレスがドメイン３０５のために電子メッセージを送信することを許可されているかどうかを判断することができる。

【００６４】

受信コンピュータシステムは、実際の送信側ネットワークアドレスを、許可サーバリストに含まれているネットワークアドレスと比較して、実際の送信側ネットワークアドレスが許可されているアドレスであるかどうかを判断することができる。例えば、メッセージサーバ３１７は、メッセージサーバ３１６に対応するネットワークアドレスを、許可サーバリスト３７８に含まれているネットワークアドレスと比較して、メッセージサーバ３１６がドメイン３０５のために電子メッセージを送信することを許可されているかどうかを判断することができる。実際の送信側ネットワークアドレスが、ドメインのための許可ネットワークアドレスのリストに含まれていない場合、これは、送信側コンピュータシステムが、そのドメインからの電子メッセージとみなされる電子メッセージを送信する許可を受けていなかったことを表す。したがって、メッセージサーバ３１６は、電子メッセージ３７１中になりすましドメイン名３７２を含めることによって、ドメイン３０５になりすましたわけであるから、メッセージサーバ３１６を不正コンピュータシステムとして認めることができる。不正コンピュータシステムによる電子メッセージの送信は、その電子メッセージが不要電子メッセージおよび／または受信者側が送信を要求していない電子メッ

セージであることを表すことができる。

【００６５】

一方、実際の送信側ネットワークアドレスがドメインのための許可ネットワークアドレスリストに含まれている場合、これは、送信側コンピュータシステムが、そのドメインからの電子メッセージとみなされる電子メッセージを送信する許可を受けていたことを表す。例えば、メッセージサーバ３１５は、電子メッセージに正当にドメイン３０５を含めることができ、許可されたコンピュータシステムとして認められる得る。許可されたコンピュータシステム（例えば、メッセージサーバ３１５）による電子メッセージの送信は、その電子メッセージが正当な電子メッセージであることを示すことができる。

【００６６】

方法４００は、判断の結果をメッセージ分類モジュールに供給する動作（動作４０５）を含む。メッセージ分類モジュールは、供給された入力に基づいて、電子メッセージを正当、不要メッセージおよび／または受信者側が送信を要求していないメッセージに分類することができる。例えば、メッセージサーバ３１７は、メッセージサーバコンピュータシステム３１６（不正）に関する、またはメッセージサーバ３１５（正当）に関する判断の結果を、メッセージ分類モジュール３２８に供給することができる。供給された、メッセージサーバ３１６が不正であることを示す結果（単独で、または他の供給された入力との組合せによる）に基づいて、メッセージ分類モジュール３２８は電子メッセージ３７１を不要メッセージおよび／または受信者側が送信を要求していないメッセージとして分類することができる。

【００６７】

実施形態によっては、メッセージ分類モジュールがメッセージクライアントに常駐している。例えば、メッセージクライアント３４３は、メッセージ分類モジュール３５３を含む。この場合、メッセージサーバ３１７は、適宜、判断（送信コンピュータシステムが、あるドメインのために電子メッセージを転送することを許可されているかどうかについての）の結果を代わりにメッセージ分類モジュール３５３に供給することができる。

【００６８】

次に図５を参照すると、図５は、本発明に従って送信ドメインの電子メッセージ送信ポリシーの識別および計算パズルの解決の確認を実施する、ネットワークアーキテクチャ５００の例を示す。ネットワークアーキテクチャには、ドメイン５０６および５０７を示してある。ドメイン５０６および５０７を、それらがそれらの内に示されている対応コンピュータシステムを論理的に含んでいることを説明するために破線で示してある。しかし、ネットワークアーキテクチャ３００と同様に、ネットワークアーキテクチャ５００のドメインに含まれるコンピュータシステムの物理的な場所は互いに異なっている。

【００６９】

ネットワークアーキテクチャ５００にはネームサーバ５０８も示してある。一般に、ネームサーバ５０８は、例えば、異なるドメインにあるコンピュータシステム間の通信を実施するために、コンピュータシステムのテキスト列識別子を対応する数値のネットワークアドレスに対応付けるネーム情報を記憶している。ネームサーバ５０８は、ドメイン名（例えば、ＷＷＷ．ｔｅｓｔ．ｃｏｍ）をインターネットプロトコル（“ＩＰ”）アドレス（例えば、１１９．４６．１２２．８７）に変換するドメインネームシステム（“ＤＮＳ”）サーバの場合がある。ネームサーバ５０８は、ドメインが１つまたは複数の電子メッセージ送信ポリシー（以下、“ＥＴＰ”と呼ぶ）を遵守していることを示すレコード、およびドメインが計算パズルの解決および／またはその解決の確認が可能であることを表すレコードも記憶することができる。

【００７０】

ＥＴＰは、例えば特別なＥＴＰレコード、ＴＸＴレコード、または１組のＴＸＴレコードなどのＤＮＳレコードに含めることができる。ＴＸＴレコードまたは１組のＴＸＴレコードは、テキストデータ、または、例えばＸＭＬ命令など、テキストフォームで符号化されたその他のデータを含むことができる。ＥＴＰを識別するレコードは、ドメインの電子

メールポリシーを表すＤＮＳレコードセット中に含めることができる。ＥＴＰは、電子メッセージポリシーに関連付けられた証拠を表す、既存の許可フレームワークおよび技術に含めることができる。例えば、ＥＴＰを、ＤＮＳレコードに記憶されているＸ．５０９証明書、拡張権利マークアップ言語（“ＸｒＭＬ”）ライセンス、またはＫｅｒｂｅｒｏｓＰＡＣに含めることができる。

【００７１】

ＥＴＰは、ドメインに対して拘束力を持つ参照テキストを含むことができ、また、相互に信頼できるソースによって発行されることができる。例えば、発行されたＸ．５０９証明書は、そのドメインに合致するルーティングアドレスを含むことができる。これは、上述のポリシーをＤＮＳから検索することよりも、ドメインに対してポリシーの拘束力を与えることになる。

【００７２】

計算パズルサポートインジケータを、例えば、特殊なパズルサポートレコード、ＴＸＴレコードまたは１組のＴＸＴレコードなどのＤＮＳレコードに含めることができる。ＴＸＴレコードまたは１組のＴＸＴレコードは、テキストデータ、または、例えばＸＭＬ命令など、テキストフォームで符号化されたその他のデータを含むことができる。計算パズルに対するサポートを表すレコードは、ドメインの電子メールポリシーを表すＤＮＳレコードに含めることができる。

【００７３】

ネットワークアーキテクチャ５００にはネットワーク５０１も示してある。ドメイン５０６、ドメイン５０７、およびネームサーバ５０８は、それぞれ、対応するリンク５９２、５９３、および５９４によってネットワーク５０１に接続されている。リンク５９２、５９３、および５９４、およびネットワーク５０１は、システムバスの一部、ローカルエリアネットワーク（“ＬＡＮ”）の一部、広域ネットワーク（“ＷＡＮ”）の一部、および／またはインターネットの一部さえも含むことができる。ネットワークアーキテクチャ５００に示してあるドメインおよびコンピュータシステムは、図示のリンクを介して、例えば、電子メールメッセージ、ＤＮＳクエリ、ＤＮＳ応答（リソースレコードを含む）などの電子メッセージを交換することができる。両方向矢印５８６で示すように、ネームサーバ５０８は、反復クエリの目的でその他のネームサーバ５８５と通信することもできる。同様に、ネットワークアーキテクチャ５００中のコンピュータシステムは、反復クエリの目的で、その他のネームサーバ５８５に直接、問い合わせることができる（ただし、ネットワークアーキテクチャ５００内のコンピュータシステムをその他のネームサーバ５８５に接続するリンクは明示していない）。

【００７４】

ドメイン５０７内において、メールクライアント５４１、５４２、および５４３は、それぞれ、対応するリンク５９６、５９７および５９８によってメッセージサーバ５１７に接続されている。メールクライアント５４１、５４２、および５４３はそれぞれ、例えば電子メールクライアントソフトウェアに含まれた、対応する電子メッセージインタフェースモジュール（図示せず）を含むことができる。電子メッセージインタフェースモジュールは、メールクライアントの１つのユーザに、電子メッセージにアクセスして見るためのメカニズムを提供する。ユーザ（例えば、Ｊａｎｅ　Ｓｍｉｔｈ）は、このユーザに割り当てられ、かつ／またはこのユーザによる使用が許可されている電子メッセージアドレス（例えば、ｊｓｍｉｔｈ＠ｔｅｓｔ１２．ｎｅｔ）に送信された電子メッセージを見ることができる。

【００７５】

図６は、本発明に従って送信ドメインの電子メッセージ送信ポリシーを判断するための方法６００の例示的流れ図を示す。電子メッセージを送信するドメインが１つまたは複数のＥＴＰを遵守している場合がある。ドメインが特定のＥＴＰを遵守していることは、そのドメインが不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージを送信する（または、他のドメインに送信させる）可能性が低いことを表す。反

対に、ドメインがその特定のＥＴＰを遵守していないことは、そのドメインが不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージを送信する（または、他のドメインに送信させる）可能性が高いことを表す。実施形態によっては、実際の送信ネットワークアドレスがハイジャックされていないことを判断した後で（例えば、方法２００に従って）、また、送信ドメインがなりすましのドメインではないことを判断した後で（例えば、方法４００に従って）、ドメインのＥＴＰを識別することが適切な場合がある。

【００７６】

方法６００を、ネットワークアーキテクチャ５００内に示す構成要素に関して説明する。方法６００は、送信ドメインから電子メッセージを受信する動作（動作６０１）を含む。動作６０１は、受信コンピュータシステムが、送信ドメインから電子メッセージ（例えば、電子メールメッセージ）を受信する動作を含むことができる。例えば、メッセージサーバ５１７は、メッセージサーバ５１６から電子メッセージ５７５（例えば、電子メールメッセージ）を受信することができる。電子メッセージ５７５は、オプションで、ドメイン５０６が遵守するＥＴＰを表すＥＴＰ証明書５７６を含む。

【００７７】

方法６００は、送信側ドメインが遵守する関連電子メッセージ送信ポリシー（例えば、特定の予め定義された標準に含まれるようなポリシー）を識別するための機能結果志向ステップ（ステップ６０５）を含む。ステップ６０５は、送信側ドメインが遵守する電子メッセージ送信ポリシーを識別するための、いずれかの対応する動作を含むことができる。しかし、図６に説明する方法では、ステップ６０５は、送信側ドメインに対応する１つまたは複数の電子メッセージ送信ポリシーを受信するという対応動作（動作６０２）を含んでいる。

【００７８】

動作６０２は、受信コンピュータシステムが、送信側ドメインに対応する１つまたは複数の電子メッセージ送信ポリシーを受信する動作を含むことができる。例えば、メッセージサーバ５１７は、ＥＴＰ証明書５７６を含む電子メッセージ５７５を受信することができる。ＥＴＰ証明書５７６は、ドメイン５０６が遵守するＥＴＰを表す、１つまたは複数のＸ．５０９証明書であり得る。

【００７９】

実施形態によっては、妥当な電子メッセージの動作のポリシーを伝達する意図で、Ｓ／ＭＩＭＥ（セキュア／マルチパーパスインターネットメールエクステンションズ）電子メッセージ（以下、「ＥＴＰ　Ｓ／ＭＩＭＥメッセージ」と呼ぶ）に署名を行う。ＥＴＰ　Ｓ／ＭＩＭＥメッセージは、Ｓ／ＭＩＭＥｖ３に準拠した電子メッセージであり得る。ＥＴＰ　Ｓ／ＭＩＭＥメッセージは、マルチパート／署名フォーマットであり得、２つのＭＩＭＥ部分を含むことができる。第１のＭＩＭＥ部分は、電子メッセージの署名すべき部分（例えば、メッセージの平文部分）を含むことができる。第２のＭＩＭＥ部分は、第１のＭＩＭＥ部分から分離された署名を含む。分離署名は、ＥＴＰ証明書の援助のもとに作成することができる。ＥＴＰ　Ｓ／ＭＩＭＥメッセージは、署名メールシステムと署名を認識しないメッセージシステムの間の改良された下位互換性を提供する、完全インヘッダモードで実装することができる。

【００８０】

電子メッセージの受信者は、自分達のＥＴＰ協約に違反するエンティティを識別することができる。したがって、電子メッセージ受信者は、ＥＴＰ　Ｓ／ＭＩＭＥ中の証明書が失効しているかどうかの判断を試みることができる。電子メッセージ受信者が証明書が失効しているかどうかの判断を試みるには少なくとも４つの方法がある。一実施形態では、電子メッセージ受信者が、証明書の発行元にその証明書が失効しているかどうかを問い合わせる。別の実施形態では、電子メッセージ受信者が、信頼できる証明書発行元によって定期的に更新される、失効証明書リストを保持する。ＥＴＰ　Ｓ／ＭＩＭＥメッセージが受信された場合、この電子メッセージの受信者は、リストをチェックして、含まれている

証明書が失効しているかどうかを判断することができる。さらに別の実施形態では、電子メッセージ受信者が、現在、委託されている全ての証明書のリストを保持する。ＥＴＰＳ／ＭＩＭＥメッセージが受信された場合、この電子メッセージの受信者は、リストをチェックして、含まれている証明書が委託されているものであるかどうかを判断することができる。

【００８１】

さらに別の実施形態では、ＥＴＰ　Ｓ／ＭＩＭＥメッセージ中に、含まれている証明書とともに新しさの証拠が含まれている。例えば、ＥＴＰ　Ｓ／ＭＩＭＥメッセージは、特定の（可能には最新の）時間枠（例えば、１分または１５分）の間、その証明書が有効な状態であることを示す、発行元からの証明書を含む。電子メッセージ受信者が、その時間枠の間に、あるいはそれよりもあまり時間が経たないうちにＥＴＰ　Ｓ／ＭＩＭＥメッセージを受信すると、その証明書は新しいとみなされる。一方、電子メッセージ受信者がその時間枠よりもかなり後にＥＴＰ　Ｓ／ＭＩＭＥを受信した場合、その電子メッセージ受信者は、例えば、証明書の発行元に問い合わせてその証明書が失効しているかどうかを知るなど、その他のメカニズムの１つに頼ることができる。

【００８２】

ＥＴＰ　Ｓ／ＭＩＭＥメッセージ中に新しさの証拠を含めることは、電子メッセージ受信者にとって効率面での多大な利点がある。例えば、ＥＴＰ　Ｓ／ＭＩＭＥ中に新しさの証拠を含めることによって、電子メール受信者が行うクエリの回数を著しく低減することができる。また、ＥＴＰ　Ｓ／ＭＩＭＥ中に新しさの証拠を含めても、伝メッセージ送信者には、与えるとしても限定的な影響しか与えない。例えば、電子メッセージの送信を、新規の新しさの証拠をたまにしか（例えば、１５分ごと）要求しないようにし、それを任意の数の電子メッセージ中に含めるように構成することができる。これによって、証明書の発行元へのクエリの回数が著しく低減される。

【００８３】

メッセージサーバ５１７はまた、送信側ドメインに対応するＥＴＰのネームサーバについてのクエリを発生させる。例えば、メッセージサーバ５１７は、ＥＴＰクエリ５８６を含む、ネームサーバメッセージ５８５を、ドメイン５０７に発行させることができる。ネームサーバメッセージ５８５は、適切なＤＮＳクエリメッセージであってよい。ネームサーバ５８５は、ドメイン５０６を識別する識別子を含むことができる。

【００８４】

ネームサーバ５０８は、ネームサーバメッセージ５８５を受信し、それに応じてＥＴＰクエリ５８６を処理することができる。ネームサーバ５０８において、エントリ５７６は、ドメイン５０６に対応するＤＮＳエントリであってよい。エントリ５７６は、証明書レコード５５６を含む、ドメイン５０６についての１つまたは複数のレコード（例えば、特別なＥＴＰレコードおよび／またはＴＸＴレコード）を含むことができる。ＴＸＴレコードまたは１組のＴＸＴレコードはＸＭＬ命令を含むことができる。証明書レコード５５６は、ドメイン５０６が遵守するＥＴＰを示す、１つまたは複数のＥＴＰ証明書（例えば、Ｘ．５０９証明書）を含むことができる。

【００８５】

ドメイン５０６が、ＥＴＰに遵守しないように構成されている場合がある。この場合、エントリ５７６は、ドメイン５０６がＥＴＰに遵守しないことを示す電子メッセージ構成情報を含む場合がある。したがって、証明書レコード５５６がどの証明書も含まない場合があり、あるいは、証明書５５６がエントリ５７６中には含まれていない場合さえある。ドメイン５０６がＥＴＰに準拠しない場合、ネームサーバ応答５１４を、ドメイン５０６がＥＴＰに準拠していないことを示すように構成することができる。したがって、ネームサーバ５０８は、ネームサーバメッセージ５８５を受信したことに応答して、ドメイン５０６がＥＴＰをサポートしないという指示とともにネームサーバ応答５１３を送信することができる。

【００８６】

一方、ドメイン５０６が、１つまたは複数のＥＴＰを遵守するように構成されている場合がある。この場合、証明書レコード５５６を、１つまたは複数のＥＴＰを含む証明書で構成することができる。したがって、ネームサーバ５０８は、ネームサーバメッセージ５８５を受信したことに応答して、ＥＴＰ証明書５１４を含むネームサーバ応答５１３をドメイン５０７に送信することができる。ドメイン５０７は、ネームサーバ応答５１３を受信して、それをメッセージサーバ５１７に転送することができる。

【００８７】

ステップ６０５は、１つまたは複数の受信電子メッセージ送信ポリシーから、関連する電子メッセージ送信ポリシーを解析する動作（動作６０３）を含む。動作６０３は、受信コンピュータシステムが、１つまたは複数の受信電子メッセージ送信ポリシーから関連電子メッセージ送信ポリシーを解析する動作を含む。例えば、メッセージサーバ５１７は、ＥＴＰ証明書５７６および／またはＥＴＰ証明書５１４から、ドメイン５０６のＥＴＰを解析することができる。ＥＴＰによっては、何が妥当なメッセージ送信動作なのかを指摘するいくつかの組織が同意している場合もある。

【００８８】

ポリシーを、特定の組織グループにとって何が適切な動作なのかに基づいて展開させることができる。しかし、いずれかの１組のポリシーを全てのメッセージユーザが例外なく遵守しなければならないということはない。ただし、例えば、電子メッセージを比較的低速で送信すること、および／または電子メッセージを多数のアドレスに送信することを控えることなど、特定のポリシーをドメインが遵守することによって、そのドメインからの電子メッセージが不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージである可能性が低いことを示すことができる。一方、これらのポリシーを遵守していないことは、そのドメインからの電子メッセージが不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージである可能性が高いことを示し得る。

【００８９】

方法６００は、関連電子メッセージ送信ポリシーをメッセージ分類モジュールに供給する動作（動作６０４）を含む。動作６０４は、受信コンピュータシステムが、関連電子メッセージ送信ポリシーをメッセージ分類モジュールに供給する動作を含むことができる。例えば、メッセージサーバ５１７は、ドメイン５０６の関連ＥＴＰをメッセージ分類モジュール５２９に供給することができる。メッセージ分類モジュール５２９は、関連ＥＴＰに基づいて（単独で、または他の供給された入力との組合せによって）、電子メッセージ５７５を正当な電子メッセージとして、または不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージとして分類することができる。代わりに、適切な場合には、メッセージサーバ５１７は、ドメイン５０６の関連ＥＴＰをメッセージ分類モジュール５５３に供給することができる。メッセージ分類モジュール５５３は、関連ＥＴＰに基づいて（単独で、または他の供給された入力との組合せによって）、電子メッセージ５７５を正当な電子メッセージとして、または不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージとして分類することができる。

【００９０】

図７は、本発明に従って計算パズルの解決を確認するための方法７００の例示的流れ図を示す。計算パズルの完了は、送信コンピュータシステムが、電子メッセージを送信する前にいくつかのプロセッササイクルを消費したことを表し得る。消費したプロセッササイクルの指示を提供することは、その送信コンピュータシステムが比較的高速で電子メッセージを送出していないことの証拠、および財源の消費の証拠となる。この場合、この送信コンピュータシステムからの電子メッセージは、不要メッセージおよび／または受信者側が送信を要求していないメッセージである可能性が潜在的に低い。

【００９１】

ネットワークアーキテクチャ５００内に示してあるコンピュータシステムおよびモジュールに関して、方法７００を説明する。方法７００は、電子メッセージに含めるべき電子

メッセージデータを受信する動作（動作７０１）を含む。動作７０１は、送信メッセージサーバまたは送信メッセージクライアントが、電子メッセージに含めるべき電子メッセージデータを受信する動作を含むことができる。メッセージデータは、電子メッセージのヘッダまたは本文部分に含めるべきいずれかのデータを含み得る。例えば、メッセージサーバ５１６に接続されたメッセージクライアントは、電子メッセージ５４５のヘッダおよび／または本文部分に含めるべきメッセージデータ（例えば、電子アドレス、件名、メッセージの本文など）を受信することができる。メッセージサーバ５１６では、電子メッセージデータがすでに配信すべき電子メッセージ（例えば、電子メッセージ５４５）に含まれている場合がある。したがって、メッセージサーバ５１６は、電子メッセージデータの部分（例えば、メッセージデータ５４６の部分）を、対応する電子メッセージが配信される前に、抽出して処理することができる。

【００９２】

計算パズルの解決を計算する前に、受信側のドメインが計算パズルの解決を確認するように構成されていることを確認することができる。例えば、受信メッセージサーバなどの受信コンピュータシステムは、それが計算パズルの解決を確認するように構成されていることを名前エントリに記入している場合がある。例えば、エントリ５７７が、ドメイン５０７の名前情報を記憶している場合がある。エントリ５７７には、ドメイン５０７が計算パズルの応答を確認するように構成されていることを示す、応答確認サポートレコード５３７がある。応答確認サポートレコード５３７は、例えば特別なパズルサポートレコード、ＴＸＴレコード、または１組のＴＸＴレコードなどのＤＮＳレコードであり得る。ＴＸＴレコードまたは１組のＴＸＴレコードは、テキストデータ、または、例えばＸＭＬ命令など、テキストフォームで符号化されたその他のデータを含む。

【００９３】

したがって、メッセージサーバ５１６は、ネームサーバコンピュータシステム５０８に問い合わせて（例えば、適切なＤＮＳクエリメッセージを送信することによって）、ドメイン５０７が計算パズルの解決を確認できるかどうかを判断することができる。このクエリに応答して、ネームサーバ５０８は、応答確認サポートレコード５３７を含む指示を返すことができ（例えば、適切なＤＮＳ応答メッセージを送信することによって）、これはドメイン５０６で受信される。ドメイン５０６は、受信した指示をメッセージサーバ５１６に適切に転送する。

【００９４】

方法７００は、状態情報の異なる部分から初期ドキュメントを生成する動作（動作７０２）を含む。動作７０２は、送信コンピュータシステムが、状態情報の異なる部分から初期ドキュメントを生成する動作を含むことができる。例えば、メッセージサーバ５１６は、メッセージデータ５４６の異なる部分から初期ドキュメントを生成することができる。実施形態によっては、メッセージデータの異なる部分から初期ドキュメントを生成する動作が、電子メッセージからメッセージデータの異なる部分を抽出する動作を含むことができる。送信メッセージサーバが、受信メッセージサーバに転送すべき電子メッセージ（例えば、メッセージクライアントからの）を受信する場合がある。例えば、メッセージサーバ５１６は、メッセージサーバ５１７に転送すべき、メッセージデータ５４６を含む電子メッセージを受信することができる。

【００９５】

メッセージサーバ５１６は、電子メッセージ５４５に含めるべきメッセージデータ５４６の部分を抽出することができる。例えば、メッセージサーバ５１６は、電子メッセージ５４５の差出人フィールド、宛先フィールド、開始時刻フィールド、終了時刻フィールド、日付フィールド、本文フィールド、添付フィールド、件名フィールド、および／またはメッセージＩＤフィールドなどに含めるべきデータの一部を抽出することができる。データの部分を抽出する動作は、例えば、テキストデータ、グラフィカルデータ、ユニフォームリソース識別子（“ＵＲＩ”）データ、実行可能データなど、実質的に、電子メッセージに含めることができるどのようなタイプのデータでも抽出する動作を含むことができる

。メッセージサーバ５１６は、次いで、抽出した部分を連結して、初期ドキュメントを生成する。

【００９６】

初期ドキュメントは、例えば、メッセージに一意のナンス（例えば、ランダムに生成された番号またはストリング）などの状態情報からも生成することができる。例えば、メッセージサーバ５１６は、１２８ビットのランダムな一意のストリングを生成して、電子メッセージ５４５に含めることができる。ナンスをメッセージデータの１つまたは複数の部分に連結して、初期ドキュメントを生成することができる。

【００９７】

方法７００は、電子メッセージの１つまたは複数の構成要素からパズル入力を生成する動作（動作７０３）を含む。動作７０３は、送信コンピュータシステムが、電子メッセージの１つまたは複数の構成要素からパズル入力を生成する動作を含むことができる。例えば、パズル計算モジュール５２８は、電子メッセージ５４５の１つまたは複数の構成要素（例えば、メッセージの本文、メッセージの添付物、およびメッセージのヘッダ）からパズル入力を生成することができる。パズル入力を生成する動作は、電子メッセージの構成要素に対する抽出、ハッシュ、連結、またはその他の動作を行うことを含むことができる。

【００９８】

実施形態によっては、パズル入力が初期ドキュメントである。別の実施形態では、パズル入力が、初期ドキュメントを初期ハッシュアルゴリズムに入力として供給することにより計算される、パズル入力ハッシュ値であり得る。初期ハッシュアルゴリズムを利用して均一な長さの入力を生成することができ、それによってより均一なパズル解決時間が得られる。初期ハッシュアルゴリズムは、応答ドキュメントを計算する場合に使用されるパズルハッシュアルゴリズムであり得る。

【００９９】

パズルハッシュアルゴリズムを、特に、不要電子メッセージおよび／または受信者側が送信を要求していない電子メッセージを阻止する際に使用するために設計することができる。例えばＳＨＡ－１アルゴリズムなどのハッシュアルゴリズムは、ハッシュ値を作成する間、入力の異なる対応部分にそれぞれ異なった時間に適用される複数の副関数を含んでいる場合がある。本発明の実施形態は、この副関数と入力の部分の間の標準的な対応を変更することによって、ハッシュアルゴリズムの標準動作を変更する。同じ副関数を利用することができるが、それらの副関数が、標準動作の場合であれば同じ部分に適用されるところを、データの異なる部分に適用される。例えば、パズルハッシュアルゴリズムは、ＳＨＡ－１アルゴリズムの副関数をハッシュすることを利用するが、それらの副関数をＳＨＡ－１アルゴリズムとは異なる順番で適用する。副関数を異なる順序で適用することにより、パズルハッシュアルゴリズムをハードウェアに実装することがより難しくなる。

【０１００】

例えば、ＳＨＡ－１が、以下の式に従って８０の副関数を指定する場合を考える。

$f_t(B,C,D)=(B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D)$ $(0 <= t <= 19)$

$f_t(B,C,D)=B \text{ XOR } C \text{ XOR } D$ $(20 <= t <= 39)$

$f_t(B,C,D)=(B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D)$ $(40 <= t <= 59)$

$f_t(B,C,D)=B \text{ XOR } C \text{ XOR } D$ $(60 <= t <= 79)$

【０１０１】

この場合、ＳＨＡ－１アルゴリズムは、以下の式に従って、８０の副関数を指定する。

$f_t(B,C,D)=B \text{ XOR } C \text{ XOR } D$ $(0 <= t <= 19)$

$f_t(B,C,D)=(B \text{ AND } C) \text{ OR } ((\text{NOT } B) \text{ AND } D)$ $(20 <= t <= 39)$

$f_t(B,C,D)=B \text{ XOR } C \text{ XOR } D$ $(40 <= t <= 59)$

$f_t(B,C,D)=(B \text{ AND } C) \text{ OR } (B \text{ AND } D) \text{ OR } (C \text{ AND } D)$ $(60 <= t <= 79)$

表１は、テキストデータの例を、それらの対応する変更済みＳＨＡ－１ハッシュ出力と共に示したものである。

【０１０２】
【表１】

テストデータ	変更済みSHA-1 ハッシュ出力
ストリング "abc"	6092C49D 8092E074 4B14298E 12E00ED2 DE4611A0
ストリング "abcdbcdecdefdefgefghfghighijhijkijkljklmklmnlmnomnopnopq"	7D3E33E1 8BB7F842 9055CB29 40BE227F CF562276
1,000,000個のaからなるストリング	21F4D548 88AF926B 9DF19A69 EC753DDD 850D7E20
空ストリング	D212F400 92F2D374 E86AB4E4 C1BE75D3 7853FDBA

表１

【０１０３】
方法７００は、応答ドキュメントとパズル入力との結合から計算された応答ハッシュ値が計算パズルの応答値になるように、応答ドキュメントを識別する動作（動作７０４）を含む。動作７０４は、送信コンピュータシステムが、応答ドキュメントとパズル入力との結合から計算された応答ハッシュ値が計算パズルの応答値になるように、応答ドキュメントを識別する動作を含むことができる。例えば、パズル計算モジュール５２８は、計算パズルの応答となる応答ハッシュ値になるような応答ドキュメントを識別することができる。
【０１０４】
一実施形態では、計算パズルは、パズル入力（例えば、初期ドキュメントまたはパズル入力ハッシュ値）と結合され、次いでパズル入力と結合された後にハッシュされた場合に（例えば、変更済みＳＨＡ－１アルゴリズムを使って）、複数のビット位置（結果として得られるハッシュ値中に散在する）に指定値を有するハッシュ値になるような応答ドキュメントを識別することである。例えば、計算パズルは、２番目のビット位置に１という値、１３番目および５４番目のビット位置にゼロの値を有するハッシュ値になるような応答ドキュメントを識別するである場合がある。しかし、本発明の実施形態は、特定の複数ビット位置または特定の指定値に限定されるものではない。
【０１０５】
より具体的な実装においては、計算パズルとは、パズル入力の先頭に追加されて、パズル入力と連結された後にハッシュされた場合に、少なくとも最初のｎビット（すなわち、各バイトの最上位ビットから始めて）がゼロであるハッシュ値になるような応答ドキュメ

ントを識別することである。例えば、計算パズルが、最初の１６ビットがゼロのハッシュ値になるような応答ドキュメントを識別することである場合がある。一般に、応答ドキュメントを識別することは、H（応答ドキュメント^{O}パズル入力）を形成することを含み得る。より具体的には、応答ドキュメントを識別することは、H（応答ドキュメント^{O}初期ドキュメント）またはH（応答ドキュメント^{O}H（初期ドキュメント））を形成することを含み得る。十分に大きいとみなされる特定の数ｎについては、強引な手段でなければ応答ドキュメントを識別できない可能性がある。

【０１０６】

計算パズルを解決する期待時間の変動を低減するために、第１の複数のビット位置（「集合Ａ」）および集合Ａ中の各ビットの指定値を選択する。集合Ａと共通のビット位置が含まれない、第２の複数のビット位置（「集合Ｂ」）も選択する。パズルの解決は、指定サイズの複数の応答ドキュメント（「集合Ｓ」）であり、この場合、各応答ドキュメントは、パズル入力と連結されてハッシュされた場合に、集合Ａ中の各ビット位置に指定値を有し、また、集合Ｂの各ビット位置の値が、１つおいた応答ドキュメントに対応するハッシュ値に一致する。

【０１０７】

変動の低減のより具体的な実施では、集合Ａが、結果として得られるハッシュ値の　プレフィックスであり、集合Ｂが、結果として得られるハッシュ値のサフィックスである。したがって、計算パズルは、各応答ドキュメントがパズル入力の先頭に追加され、次いで各応答ドキュメントとパズル入力との連結がハッシュされた場合に、少なくとも最初のｎビット（集合Ａ）がゼロであり、最後のｍビット（集合Ｂ）が同一の値であるような集合Ｓを識別することの場合がある。例えば、計算パズルは、最初の２４ビットがゼロであり、最後の１２ビットが同じ値（０か１）であるハッシュ値になる、１６の応答ドキュメントを識別することであり得る。代わりに、最初の２４ビットおよび／または最後の１２ビットが、ゼロの値と１の値を散在させた指定のビットパターンのこともあり得る。

【０１０８】

計算パズルを解決するための期待時間を、集合Ａ、集合Ｂ、および／または集合Ｓのサイズを変えることによって構成することができる。集合Ａのサイズを、適切な期待解決時間が得られるように変えることができる。集合Ｂのサイズおよび集合Ｓのサイズを変化させて、適切に解決時間を変えることができる。解決時間がより長くなるように計算問題を構成することによって、それに応じて、解決を識別するために消費される計算リソースが増加する。一方、解決時間がより短くなるように計算問題を構成することによって、それに応じて、解決を識別するために消費される計算リソースが減少する。メッセージサーバ（例えば、サーバ５１６および５１７）は、指定の解決時間に同意することによって、または、対応するリソースレコードに問い合わせることによって、指定解決時間を識別することができる。例えば、メッセージサーバ５１６は、エントリ５７７に問い合わせて、ドメイン５０７の特定の解決時間を識別することができる。

【０１０９】

実施形態によっては、一方向パズルハッシュ関数が利用される。一方向パズルハッシュ関数が、特に、不要電子メッセージおよび／または受信者側が送信を要求していな電子メッセージを阻止する際に使用するために設計されている場合がある。一方向パズルハッシュ関数は、ハードウェアの加速を防ぐ目的で、既知の一方向ハッシュを変更したものであり得る。より詳細には、一方向パズルハッシュ関数は、著しい回数の除算を含む。除算は、ハードウェアで加速することが困難なためである。

【０１１０】

送信コンピュータシステムは、識別された応答ドキュメント（または識別された複数の応答ドキュメント）を、電子メッセージデータと共に電子メッセージに含めることができる。例えば、メッセージサーバ５１６は、応答ドキュメント５４７を、メッセージデータ５４６と共に電子メッセージ５４５（例えば、電子メールメッセージ）に含めることができる。方法７００は、識別された応答ドキュメントおよび電子メッセージデータを含む電

子メッセージを、受信側ドメインに送信する動作（動作７０５）を含む。動作７０５は、送信コンピュータシステムが、識別された応答ドキュメント（または応答ドキュメント）および電子メッセージデータを含む電子メッセージを、受信側ドメインに送信する動作を含むことができる。例えば、メッセージサーバ５１６は、応答ドキュメント５４７およびメッセージデータ５４６を含む電子メッセージ５４５を、ドメイン５０７に送信することができる。ドメイン５０７は、電子メッセージ５４５をメッセージサーバ５１７に転送することができる。電子メッセージ５４５を単一の応答ドキュメント（応答ドキュメント５４７）を含むものとして示してあるが、電子メッセージ５４５は、１つまたは複数のさらなる応答ドキュメントを含む場合がある。

【０１１１】

方法７００は、電子メッセージデータおよび応答ドキュメントを含む電子メッセージを受信する動作（動作７０６）を含む。動作７０６は、受信コンピュータシステムが、電子メッセージデータおよび応答ドキュメント（または応答ドキュメント）を含む電子メッセージを受信する動作を含むことができる。例えば、メッセージサーバ５１７は、応答ドキュメント５４７およびメッセージデータ５４６を含む電子メッセージ５４５を受信することができる。電子メッセージが特定のメッセージクライアントに配信される場合、メッセージサーバは、電子メッセージをそのメッセージクライアントに転送することができる。例えば、メッセージサーバ５１７は、適切な場合には、電子メッセージ５４５をメッセージクライアント５４２に転送することができる。メッセージクライアント５４２は、電子メッセージ５４５を受信することができる。

【０１１２】

方法７００は、状態情報の異なる部分から初期ドキュメントを再生する動作（動作７０７）を含む。動作７０７は、受信コンピュータシステムが、状態情報の異なる部分から初期ドキュメントを再生する動作を含むことができる。例えば、応答確認モジュール５２７および／または応答確認モジュール５５２は、電子メッセージ５４５（例えば、ナンス）に含まれるメッセージデータ５４６またはその他の状態情報の部分から、初期ドキュメントを再生することができる。初期ドキュメントの計算と同様に、応答確認モジュール５２７および／または応答確認モジュール５５２は、メッセージデータ５４６またはその他の状態情報の部分を抽出して連結し、初期ドキュメントを再生することができる。

【０１１３】

方法７００は、電子メッセージの１つまたは複数の構成要素からパズル入力を再計算する動作（動作７０８）を含む。パズル入力を再計算することにより、初期ドキュメント、または送信コンピュータシステムで使用したのと同じパズルハッシュアルゴリズム（例えば、変更済みＳＨＡ－１アルゴリズム）を使って計算されたパズル入力ハッシュ値にすることができる。例えば、応答確認モジュール５２７および／または応答確認モジュール５５２は、パズル計算モジュール５２８が使用したのと同じパズルハッシュアルゴリズムを使って、再生された初期ドキュメントからパズル入力ハッシュ値を再計算することができる。この場合、送信コンピュータシステムにおいて計算されたパズル入力が、受信コンピュータシステムにおいて再計算される。

【０１１４】

方法７００は、応答ドキュメントとパズル入力との結合から計算された確認ハッシュ値が、計算パズルの解決を表す応答値であるかどうかを判断する動作（動作７０９）を含む。動作７０９は、受信コンピュータシステムが、応答ドキュメントとパズル入力との結合から計算された確認ハッシュ値が計算パズルの解決を表す応答値であるかどうかを判断する動作を含むことができる。例えば、応答確認モジュール５２７および／または応答確認モジュール５５２は、一般的公式Ｈ（応答ドキュメント○パズル入力）を利用して、確認ハッシュ値が解決を表しているかどうかを判断することができる。確認ハッシュ値が、その中に散在する複数の固定ビット位置（例えば、最初のｎビット）に指定値を持つ場合、その確認ハッシュ値は解決を表していると言える。

【０１１５】

実施形態によっては、複数の応答ドキュメントおよびパズル入力との結合から、複数の確認ハッシュ値が算出される。これらの実施形態では、確認ハッシュ値が、第１の複数のビット位置（例えば、ハッシュ値のプレフィックス）に指定値を有し、第２の複数のビット位置（例えば、ハッシュ値のサフィックス）に、その他の応答ドキュメントから得られたその他の確認ハッシュ値に等しい値を有する場合、その確認ハッシュ値は解決を表していると言える。

【０１１６】

確認ハッシュ値が計算問題の解決である場合、消費された計算リソースを少なくとも見積もることができる。すなわち、計算パズルに対する確認可能な解決によって、受信コンピュータシステムは、送信コンピュータシステムがその計算パズルを解決するために強引なアプローチでプロセッササイクルおよびメモリリソースを消費したことを知ることができる。例えば、確認ハッシュ値がメッセージデータ５４６に基づく計算パズルの解決である場合、これは、メッセージサーバ５１６がプロセッササイクルを消費したことを応答確認モジュール５２７および／または応答確認モジュール５５２に示す。一方、確認ハッシュ値が計算問題の解決ではない場合、これは、その送信コンピュータシステムが、計算パズルを解決するために強引なアプローチでプロセッササイクルを消費しなかった可能性が高いことを表す。例えば、確認ハッシュ値がメッセージデータ５４６に基づいた計算パズルの解決ではない場合、これは、メッセージサーバ５１６がプロセッササイクルを消費しなかった可能性が高いことを、応答確認モジュール５２７および／または応答確認モジュール５５２に示す。

【０１１７】

方法７００は、判断の結果をメッセージ分類モジュールに供給する動作（動作７１０）を含む。動作７１０は、受信コンピュータシステムが、判断の結果をメッセージ分類モジュールに供給する動作を含むことができる。例えば、メッセージサーバ５１７は、メッセージサーバ５１６に関する判断の結果（メッセージサーバ５１６がプロセッササイクルを消費した、または消費しなかったことを示す判断の結果）をメッセージ分類モジュール５２９に供給することができる。供給された、メッセージサーバ５１６が計算リソースを消費したことを示す判断に基づいて（単独で、または他の供給された入力との組合せによって）、メッセージ分類モジュール５２９は、電子メッセージ５４５を正当なメッセージとして分類することができる。一方、供給された、メッセージサーバ５１６が計算リソースを消費しなかった可能性が高いことを示す判断に基づいて（単独で、または他の供給された入力との組合せによって）、メッセージ分類モジュール５２９は電子メッセージ５４５を不要メッセージおよび／または受信者側が送信を要求していないメッセージとして分類することができる。代わりに、適切な場合には、メッセージサーバ５１７は、メッセージサーバ５１６が計算リソースを消費した、または消費しなかった可能性が高いことを示す結果をメッセージ分類モジュール５５３に供給することができる。

【０１１８】

本発明の実施形態によっては、ドメインが指定ＥＴＰをサポートするという指示または送信コンピュータシステムが計算パズルを解決したという指示のいずれかが、電子メッセージが正当であることの十分な証拠になる。例えば、送信エンティティが財源、またはＥＴＰ証明書を利用したいという要望が不足している場合がある。しかし、それでも、この送信エンティティが、電子メッセージが正当であることを受信コンピュータシステムに示したいと思う場合がある。この場合、送信エンティティは、計算パズルの解決を計算して、電子メッセージに応答ドキュメントを含めるように送信コンピュータシステムを構成することができる。

【０１１９】

そのような送信エンティティに関連するドメインのＥＴＰ証明書の識別を試みるように、受信コンピュータシステムを構成することができる。さらに、ＥＴＰ証明書が１つも識別されなかった場合には計算パズルの解決を確認するように、受信コンピュータシステムを構成することができる。この場合、受信コンピュータシステムは、最初に電子メッセー

ジを解析し、または送信エンティティに関連するドメインに対応するＥＴＰ証明書をネームサーバに問い合わせる。ＥＴＰ証明書が識別され、そのＥＴＰ証明書が特定のＥＴＰに対するサポートを示す場合、その特定のＥＴＰに対するサポートは、電子メッセージが正当であることの十分な証拠となり得る。しかし、ＥＴＰ証明書が１つも識別されない場合、または、識別されたＥＴＰ証明書が特定のＥＴＰに対するサポートを示していない場合、受信コンピュータシステムは、引き続き、含まれている計算パズルの解決の確認を試みる。

【０１２０】

スキーマを使って、電子メッセージ情報の意味に制約を与えることができる。以下の例示的ＸＭＬスキーマを使って、ドメインに関連する電子メッセージ情報の意味に制約を与えることができる。

【０１２１】

【表２】

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="http://lessspam.org/1" xmlns="http://lessspam.org/1"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="unqualified" blockDefault="#all">
  <xs:element name="emailPolicy">
    <xs:complexType>
```

【０１２２】

【表３】

```
<xs:sequence>
  <xs:element name="inbound" minOccurs="0">
    <xs:annotation>
      <xs:documentation>Policies regarding mail that is received by the entity.
      </xs:documentation>
    </xs:annotation>
    <xs:complexType>
      <xs:choice minOccurs="0" maxOccurs="unbounded">
        <xs:element name="hashedSpam">
          <xs:complexType>
            <xs:attribute name="minDifficulty" type="xs:nonNegativeInteger">
              <xs:annotation>
                <xs:documentation>The minimum acceptable level of difficulty
in
                    the puzzle solution.
                </xs:documentation>
              </xs:annotation>
            </xs:attribute>
            <xs:attribute name="maxIntervalWidth" type="xs:duration">
              <xs:annotation>
                <xs:documentation>The maximum acceptable width of the time
                    interval parameter of the puzzle.
                </xs:documentation>
              </xs:annotation>
            </xs:attribute>
            <xs:attribute name="dateRequired" type="xs:boolean"
default="false">
              <xs:annotation>
                <xs:documentation>Whether a the inclusion of a date parameter
is
                    required (it is always acceptable if present).
                </xs:documentation>
```

【０１２３】

【表４】

```
                </xs:annotation>
              </xs:attribute>
              <xs:attribute name="subjectRequired" type="xs:boolean"
                    default="false">
                <xs:annotation>
                  <xs:documentation>Whether a the inclusion of a subject
parameter
                    is required (it is always acceptable if present).
                  </xs:documentation>
                </xs:annotation>
              </xs:attribute>
              <xs:anyAttribute namespace="##other" processContents="lax"/>
            </xs:complexType>
          </xs:element>
          <xs:any namespace="##other" processContents="lax"/>
        </xs:choice>
      </xs:complexType>
    </xs:element>
    <xs:element name="outbound" minOccurs="0">
      <xs:annotation>
        <xs:documentation>Policies regarding mail that is sent from the entity.
        </xs:documentation>
      </xs:annotation>
      <xs:complexType>
        <xs:choice minOccurs="0" maxOccurs="unbounded">
          <xs:element name="mailServer">
            <xs:annotation>
              <xs:documentation>One group of outbound mail servers. The
                  usesEnhancedSMTPNoop attribute, if present indicates their
known
                  behaviour with respect to that feature.
              </xs:documentation>
```

【０１２４】

【表５】

```
            </xs:annotation>
            <xs:complexType>
              <xs:choice minOccurs="0">
                <xs:element name="indirect" type="xs:string">
                  <xs:annotation>
                    <xs:documentation>An indirection to another domain.
                    </xs:documentation>
                  </xs:annotation>
                </xs:element>
                <xs:choice maxOccurs="unbounded">
                  <xs:element name="address" type="xs:string"/>
                  <xs:element name="addressV6" type="xs:string"/>
                  <xs:element name="addressRange" type="xs:string"/>
                </xs:choice>
              </xs:choice>
              <xs:attribute name="usesEnhancedSmtpNoop" type="xs:boolean"
                    use="optional"/>
              <xs:attribute name="allMailIsETPSigned" type="xs:boolean"
                    use="optional"/>
              <xs:anyAttribute namespace="##other" processContents="lax"/>
            </xs:complexType>
          </xs:element>
          <xs:any namespace="##other" processContents="lax"/>
        </xs:choice>
      </xs:complexType>
    </xs:element>
    <xs:element name="otherInfo" minOccurs="0">
      <xs:annotation>
        <xs:documentation>General other information regarding the entity, such
as
            certificates that may pertain to it.
          </xs:documentation>
```

【０１２５】

【表６】

```
            </xs:annotation>
            <xs:complexType>
              <xs:choice minOccurs="0" maxOccurs="unbounded">
                <xs:element name="x509Certificate" type="xs:base64Binary"/>
                <xs:any namespace="##other" processContents="lax"/>
              </xs:choice>
            </xs:complexType>
          </xs:element>
        </xs:sequence>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
      </xs:complexType>
    </xs:element>
    <xs:element name="ocspResponse" type="xs:base64Binary">
      <xs:annotation>
        <xs:documentation>Base64 encoding of an RFC2560 OCSPResponse.
        </xs:documentation>
      </xs:annotation>
    </xs:element>
  </xs:schema>
```

【０１２６】

スキーマを使用することによって、開発者は、電子メッセージ構成情報を処理するアプリケーションを再設計する必要なく、電子メッセージ構成情報をどのように構造化するかを柔軟に定義することができる（あるいは再定義することさえできる）。ＴＸＴレコードを利用して、例示のＸＭＬスキーマによって制約を与えたＸＭＬ命令を記憶することができる。ＸＭＬ命令は、同じＤＮＳレコードセット中の複数のＴＸＴレコードにわたることが可能であり、そのＤＮＳレコードセットを受信したコンピュータシステムにおいてＸＭＬインスタンスにまとめることができる。例えば、各ＴＸＴレコードは、複数のＴＸＴレコードに一意の非負整数である、十進法表示の４桁を含む４文字で（必要に応じて先頭にゼロを用いて）開始することが可能である。受信されると、このＴＸＴレコードは十進数順に順序付けられる。各ＴＸＴレコードから最初の４文字（十進数）が取り除かれ、その結果得られた文字が連結されて、単一の連続した文字列（ＸＭＬインスタンス）が形成される。

【０１２７】

以下は、ドメインのＸＭＬポリシードキュメントを示す、例示的ＤＮＳ構成ファイルフラグメントである。

【０１２８】

【表７】

```
_emailPolicy TXT ("0002T0H45M0S'/>"
                  "    <hashedSpam minDifficulty='13'
                       maxIntervalWidth='P0Y0M7DT0H0M0S'"
                  "     dateRequired='true' subjectRequired='true'/>"
                  "  </inbound>"
                  "</emailPolicy>" )
            TXT ("0001<emailPolicy xmlns='http://lessspam.org/1'>"
                  "  <inbound>"
                  "    <hashedSpam minDifficulty='13' maxIntervalWidth='P0Y0M0D" )
```

【０１２９】

この例示的ＤＮＳ構成ファイルフラグメントは、２つのＴＸＴレコードを含む。１つは文字列“０００２”を含み、もう１つは文字列“０００１”を含む。受信コンピュータシステムでは、これらの文字列を使ってＴＸＴレコードに含まれるＸＭＬ命令の適切な順序を判断することができる。しかし、当業者には、この説明を検討することにより、その他の順序メカニズムを使用することが可能であり、また、ＤＮＳ構成ファイルがさらなるＴＸＴレコードを含み得ることが明らかであろう。コンピュータシステムではこれらの２つのテキストレコードを受信することができ（例えば、ＤＮＳクエリに応答して）、また、ＴＸＴレコードの部分を連結してＸＭＬインスタンスにすることができる。ＸＭＬインスタンスを複数のＴＸＴレコードに及ぶようにすることによって、より多量の電子メッセージ構成情報（２０００文字を超える情報）を運ぶことが可能になる。さらに、ＸＭＬインスタンスの異なる部分を同じＤＮＳレコードセットに含めることができるので、１つのＤＮＳクエリで異なる部分を検索することができる。

【０１３０】

この例示的ＤＮＳ構成ファイルフラグメントまたはその他のＤＮＳ構成ファイルフラグメントを、ＤＮＳサブドメイン（例えば、＿ｅｍａｉｌＰｏｌｉｃｙサブドメイン）に含めることができる。したがって、電子メッセージ構成情報を含む１つまたは複数のＴＸＴレコード（例えば、例示的ＤＮＳ構成ファイルフラグメントのＴＸＴレコード）が、特定のＤＮＳサブドメイン内のレコードの全てである場合がある。したがって、既存のＴＸＴレコード（他のサブドメイン中の）の使用との混乱またはコンフリクトを低減することができる。

【０１３１】

以下は、例示的ＤＮＳ構成ファイルフラグメントの部分を連結した結果得られる、例示的ＸＭＬインスタンスである。

【０１３２】

【表８】

```
<?xml version="1.0" encoding="UTF-8"?>
<emailPolicy xmlns="http://lessspam.org/1">
    <inbound>
        <hashedSpam minDifficulty="13"
maxIntervalWidth="P0Y0M0DT0H45M0S"/>
        <hashedSpam minDifficulty="29"
maxIntervalWidth="P0Y0M7DT0H0M0S"
                dateRequired="true" subjectRequired="true"/>
    </inbound>
</emailPolicy>
```

【０１３３】

例示的ＸＭＬインスタンスは、例示的ＸＭＬスキーマによって制約を受けたｅｍａｉｌＰｏｌｉｃｙエレメントを含む。例示的ＸＭＬインスタンスは、ＨａｓｈｅｄＳｐａｍ計算パズルに関する２つの受信ポリシーを表している。第１の受信ポリシーは、少なくとも１３のゼロビットを有し、また４５分間以下の時間間隔パラメータを有するパズル解決が受諾可能であることを示している。第２の受信ポリシーは、少なくとも２９のゼロビットを有し、１週間以内の時間間隔パラメータ、指定された日付および件名ヘッダを有するパズル解決も受諾可能であることを示している。

【０１３４】

ネームサーバで、例示的ＸＭＬインスタンスの部分、およびその他のＸＭＬインスタンスをＴＸＴレコードに含めることにより、ドメインまたは電子メッセージサーバに関連する電子メッセージ構成情報を伝達することができる。例えば、このようなＸＭＬインスタンスは、変更済み接続確立データに対するサポート、許可送信メールサーバ、ＥＴＰ証明書の参照、および計算パズルに対するサポートを伝達することができる。ＸＭＬインスタンスの部分をＴＸＴレコードに含めることによって、クライアントおよび／またはサーバＤＮＳソフトウェアを更新する必要なく、新しいタイプの電子メッセージ情報をＤＮＳに追加することもできる。

【０１３５】

ネームサーバを、電子メッセージ構成情報を返す場合に連番を要求するプロトコルを利用するように、明確に構成する場合がある。この場合、ネームサーバのなりすましを試みようとすると、そのネームサーバが使用している連番を当てなければならないというさらなる負担がかけられる。例えば、ネームサーバを、ユーザデータグラムプロトコル（“ＵＤＰ”）ではなくＴＣＰを介して電子メッセージ構成情報を返すように、明確に構成することができる。この場合、ネームサーバのなりすましを試みようとすると、そのネームサーバが使用している適切なＴＣＰ／ＩＰ連番を当てることが要求される。実施形態によっては、電子メッセージ構成情報の長さが返される結果として、連番を要求するプロトコルが使用される。例えば、ＸＭＬインスタンスが５１２バイトよりも大きい場合、自動的にＴＣＰが使用される。

【０１３６】

電子メッセージ送信側が、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージを減らすためのメカニズムを複数利用するように構成されている場合がある。この場合、この電子メッセージ送信側は、電子メッセージを送信する場合に、構成されているメカニズムのうちの１つ、いくつか、または全てを選択することができる。同様

に、電子メッセージ受信側が、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージを減らすためのメカニズムを複数利用するように構成されている場合がある。この場合、この電子メッセージ受信側は、電子メッセージを受信する場合に、構成されているメカニズムのうちの１つ、いくつか、または全てを選択することができる。しかし、電子メッセージ送信側の構成メカニズムが電子メッセージ受信側の構成メカニズムとは異なる場合がある。

【０１３７】

したがって、電子メッセージ送信側および受信側は、不要電子メッセージおよび受信者側が送信を要求していない電子メッセージを減らすための双方で構成されたメカニズムに同意する場合がある。この場合、異なって構成されたメカニズムからの結果を結合したものが、メッセージ分類モジュールに供給される場合がある。例えば、電子メッセージの受信側は、ＥＰＴへの遵守に対するチェックと、電子メッセージ送信側による努力の証拠に対するチェックの両方を行って、その両方のチェックの結果をメッセージ分類モジュールに供給する場合がある。努力の証拠には、ハッシュの衝突、暗号化の問題に対する解決策、メモリの制約の問題に対する解決策、逆チューリングテストに対する解決策を提供することが含まれ得る。受信側のドメインは、提供された努力の証拠をチェックして、チェックの結果をメッセージ分類モジュールに提供することができる。

【０１３８】

この説明、および添付の特許請求の範囲では、「スキーマ」を、複数のコンピュータシステムがそれに従ってドキュメントを処理することを可能にする、それらの複数のコンピュータシステム間の共用ボキャブラリの表現として定義している。例えば、拡張マークアップ言語（“ＸＭＬ”）スキーマは、ＸＭＬスキーマ言語のスキーマコンストラクトを使って、ＸＭＬドキュメントのクラスを定義および記述することができる。これらのスキーマコンストラクトを使って、データ型の意味、使用法および関係、エレメントおよびそれらの内容、属性およびそれらの値、エンティティおよびそれらの内容、および表記法を、ＸＭＬドキュメント中で使用するように制約を与え、また文書化する。したがって、ＸＭＬスキーマにアクセス可能であればどのコンピュータシステムでも、ＸＭＬスキーマに従ってＸＭＬドキュメントを処理することができる。さらに、ＭＬスキーマにアクセス可能であればどのコンピュータシステムでも、同じくＸＭＬスキーマにアクセス可能なその他のコンピュータシステムが使用できるように、ＸＭＬドキュメントを作成または修正することができる。

【０１３９】

所望の機能に応じて、複数の異なる生成入力のうちの１つまたは複数を、可能には電子メッセージに含まれたメッセージデータと共に、メッセージ分類モジュールに供給することができる。受信した入力に基づいて、メッセージ分類モジュールは、電子メッセージを正当なメッセージ、または不要メッセージおよび／または受信者側が送信を要求していないメッセージとして分類することができる。複数の入力（各入力が電子メッセージの送信に関連する情報を表す）を利用する場合、メッセージ分類モジュールは、例えば、電子メッセージを不要メッセージおよび／または受信者側が送信を要求していないメッセージとしてより信頼性高く分類するなど、電子メッセージをより信頼性高く分類することができる。

【０１４０】

当業者は、本発明が、パーソナルコンピュータ、ラップトップコンピュータ、ハンドヘルドデバイス、マルチプロセッサシステム、マイクロプロセッサベースの、またはプログラム可能な家庭用電子機器、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、携帯電話、ＰＤＡ、ページャなどを含む様々なタイプのコンピュータシステム構成を備えたネットワークコンピューティング環境において実施できることを理解されよう。本発明はまた、ネットワークを介してリンクされた（有線データリンク、無線データリンクによって、または有線データリンクと無線データリンクの組合せによって）ローカルおよびリモートのコンピュータシステムが共にタスクを実行する分散システム環境にお

いても、実施することができる。分散システム環境においては、プログラムモジュールをローカルおよびリモートのメモリ記憶装置の両方に設置することができる。

【０１４１】

図８および以下の説明は、本発明を実施することができる適切なコンピューティング環境の簡単かつ一般的な説明を提供することを目的としている。必ずしも必要とされるわけではないが、本発明を、コンピュータシステムによって実行されている、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という一般的な状況において説明する。一般に、プログラムモジュールは、特定のタスクを実行し、また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、構成要素、データ構造などを含む。コンピュータ実行可能命令、関連するデータ構造、およびプログラムモジュールは、本明細書に開示する方法の動作を実行するためのプログラムコード手段の例を示す。

【０１４２】

図８を参照すると、本発明を実施するための例示的システムは、処理装置８２１、システムメモリ８２２、およびシステムメモリ８２２を含む様々なシステム構成要素を処理装置８２１に結合するシステムバス８２３を含む、コンピュータシステム８２０の形態の汎用コンピューティングデバイスを含む。処理装置８２１は、本発明の機能を含む、コンピュータシステム８２０の機能を実装するように設計された、コンピュータ実行可能命令を実行することができる。システムバス８２３は、様々なバスアーキテクチャのいずれかを使用した、メモリバスまたはメモリコントローラ、周辺バス、およびローカルバスを含む、いくつかのタイプのバス構造のうちのいずれかであってよい。システムメモリは、読取り専用メモリ（“ＲＯＭ”）８２４およびランダムアクセスメモリ（“ＲＡＭ”）８２５を含む。起動時などにコンピュータシステム８２０内のエレメント間における情報の転送を援助する基本ルーチンを含む、基本入出力システム（“ＢＩＯＳ”）８２６を、ＲＯＭ８２４に記憶することができる。

【０１４３】

コンピュータシステム８２０はまた、磁気ハードディスク８３９からの読取りおよびそこへの書込みを行うための磁気ハードディスクドライブ８２７、リムーバブル磁気ディスク８２９からの読取りおよびそこへの書込みを行うための磁気ディスクドライブ８２８、例えばＣＤ－ＲＯＭやその他の光媒体などのリムーバブル光ディスク８３１からの読取りおよびそこへの書込みを行うための光ディスクドライブ８３０も含むことができる。磁気ハードディスクドライブ８２７、磁気ディスクドライブ８２８、および光ディスクドライブ８３０は、それぞれ、ハードディスクドライブインタフェース８３２、磁気ディスクドライブインタフェース８３３、および光ドライブインタフェース８３４によってシステムバス８２３に接続されている。ドライブおよびそれらに関連するコンピュータ読取り可能媒体は、コンピュータ実行可能命令、データ構造、プログラムモジュール、およびその他のデータの不揮発性記憶をコンピュータシステム８２０に提供する。本明細書に記載の例示的環境は、磁気ハードディスク８３９、リムーバブル磁気ディスク８２９、およびリムーバブル光ディスク８３１を利用しているが、磁気カセット、フラッシュメモリカード、ディジタル多用途ディスク、ベルヌーイカートリッジ、ＲＡＭ、ＲＯＭなどを含めて、データを記憶するためのその他のタイプのコンピュータ読取り可能媒体を使用することもできる。

【０１４４】

オペレーティングシステム８３５、１つまたは複数のアプリケーションプログラム８３６、その他のプログラムモジュール８３７、およびプログラムデータ８３８を含めて、１つまたは複数のプログラムモジュールを含むプログラムコード手段を、ハードディスク８３９、磁気ディスク８２９、光ディスク８３１、ＲＯＭ８２４またはＲＡＭ８２５に記憶することができる。ユーザは、キーボード８４０、ポインティングデバイス８４２、またはマイクロフォン、ジョイスティック、ゲームパッド、スキャナなど、その他の入力デバイス（図示せず）を介して、コンピュータシステム８２０にコマンドおよび情報を入力することができる。これらおよびその他の入力デバイスを、システムバス８２３に結合され

た入出力インタフェース８４６を介して、処理装置８２１に接続することができる。入出力インタフェース８４６は、例えば、シリアルポートインタフェース、ＰＳ／２インタフェース、パラレルポートインタフェース、ユニバーサルシリアルバス（“ＵＳＢ”）インタフェース、または電気電子技術者協会（ＩＥＥＥ）１３９４インタフェース（すなわち、ＦｉｒｅＷｉｒｅインタフェース）などの広範にわたる様々な異なるインタフェースのいずれかを論理的に表し、あるいは、さらに、異なるインタフェースの組合せを論理的に表す場合もある。

【０１４５】

モニタ８４７またはその他のディスプレイデバイスも、ビデオインタフェース８４８を介してシステムバス８２３に接続されている。スピーカ８６９またはその他のオーディオ出力デバイスも、オーディオインタフェース８４９を介してシステムバス８２３に接続されている。例えばプリンタなどのその他の周辺出力デバイス（図示せず）も、コンピュータシステム８２０に接続することができる。

【０１４６】

コンピュータシステム８２０は、例えば、オフィス規模または企業規模のコンピュータネットワーク、家庭内ネットワーク、イントラネット、および／またはインターネットなどのネットワークに接続可能である。コンピュータシステム８２０は、このようなネットワークを介して、例えばリモートコンピュータシステム、リモートアプリケーションおよび／またはリモートデータベースなどの外部ソースと、データを交換することができる。例えば、コンピュータシステム８２０は、コンピュータシステム８２０と共通のネットワークに接続されたその他のコンピュータシステムと電子メッセージを交換することができる。

【０１４７】

コンピュータシステム８２０はネットワークインタフェース８５３を含み、これを介して、外部ソースからデータを受信し、かつ／または外部ソースにデータを送信する。図８に示すように、ネットワークインタフェース８５３は、リンク８５１を介してリモートコンピュータシステム８８３とのデータの交換を実施する。ネットワークインタフェース８５３は、例えばネットワークインタフェースカードおよび対応するネットワークドライバインターフェース規約（“ＮＤＩＳ”）スタックなどの、１つまたは複数のソフトウェアおよび／またはハードウェアモジュールを論理的に表し得る。データリンク８５１は、ネットワークの一部（例えば、イーサネット（登録商標）セグメント）を表し、リモートコンピュータシステム８８３はネットワークのノードを表す。例えば、リモートコンピュータシステム８８３は、コンピュータシステム８２０にＤＮＳクエリを送信する問合せコンピュータシステムであり得る。一方、リモートコンピュータシステム８８３は、ＤＮＳクエリを受信したことに応答して、コンピュータシステム８２０にＤＮＳ応答を送信するＤＮＳサーバであり得る。

【０１４８】

同様に、コンピュータシステム８２０は入出力インタフェース８４６を含み、それを介して外部ソースからデータを受信し、かつ／または外部ソースにデータを送信する。入出力インタフェース８４６は、データリンク８５９を介してモデム５５４（例えば、標準モデム、ケーブルモデム、ディジタル加入者回線（“ＤＳＬ”）モデム）に結合されており、それを通してデータを受信し、かつ／または外部ソースにデータを送信する。図８に示すように、入出力インタフェース８４６およびモデム８５４は、リンク８５２を介して、リモートコンピュータシステム８９３とのデータの交換を実施する。リンク８５２はネットワークの一部を表し、リモートコンピュータシステム８９３はネットワークのノードを表す。例えば、リモートコンピュータシステム８９３は、電子メッセージをコンピュータシステム８２０に送信する送信コンピュータシステムの場合がある。一方、リモートコンピュータシステム８９３は、コンピュータシステム８２０から電子メールメッセージを受信する受信コンピュータシステムの場合がある。

【０１４９】

図８は、本発明のための適切な動作環境を表すが、本発明の原理は、必要に応じて適切な変更を加えて本発明の原理を実施することができる、どのシステムにおいても利用することができる。図８に示す環境は例にすぎず、本発明の原理を実施することが可能な広範にわたる様々な環境のわずかな部分を表すものでさえない。

【０１５０】

本発明を、その趣旨または基本的な特性から逸脱することなく、その他の特定の形態で実施することができる。記載の実施形態は、あらゆる点に関して、例示的なものにすぎず、限定的なものではないとみなすべきものとする。したがって、本発明の範囲は、上述の説明によってではなく、添付の特許請求の範囲によって示される。特許請求の範囲の同等物の意味および範囲に含まれるあらゆる変更は、特許請求の範囲に含まれるものとする。

【図面の簡単な説明】

【０１５１】

【図１】本発明の原理に従って接続ハイジャックの低減を実施するネットワークアーキテクチャの一例を示す図である。

【図２】本発明の原理に従って接続ハイジャックを低減するための方法の例示的流れ図である。

【図３】本発明に従って許可された送信メッセージサーバの識別を実施する、ネットワークアーキテクチャの一例を示す図である。

【図４】本発明に従って許可された送信メッセージサーバを識別するための方法の例示的流れ図である。

【図５】本発明に従って送信ドメインの電子メッセージ送信ポリシーの判断、および計算パズルの解決の確認を実施する、ネットワークアーキテクチャの一例を示す図である。

【図６】本発明に従って送信ドメインの電子メッセージ送信ポリシーを判断するための方法の例示的流れ図である。

【図７】本発明に従って計算パズルの解決を確認するための方法の例示的流れ図である。

【図８】本発明の原理に適した動作環境を示す図である。

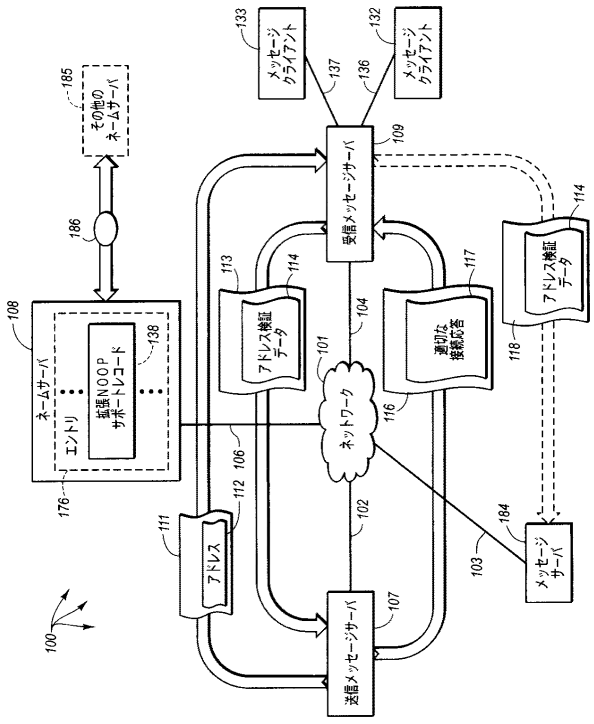
【符号の説明】

【０１５２】

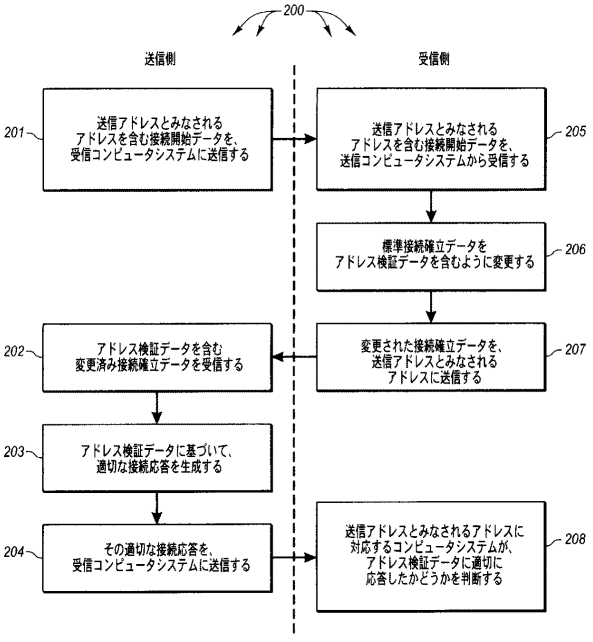
１００、３００、５００　ネットワークアーキテクチャ
１０１、３０１、５０１　ネットワーク
１０２、１０３、１０４、１０６、１３６、１３７、３９１、３９２、３９３、３９４、３９６、３９７、５９２、５９３、５９４、５９６、５９７、５９８　リンク
１０６、３０５、３０６、３０７、５０６、５０７　ドメイン
１０７　送信メッセージサーバ
１０８、３０８、３８５、５０８、５８５　ネームサーバ
１０９　受信メッセージサーバ
１１１、１１３、１１８　接続開始データ
１１２　アドレス
１１４　アドレス検証データ
１１６、１１７　接続応答データ
１３２、１３３、３４１、３４３、５４２　メッセージクライアント
１３８　拡張ＮＯＯＰサポートレコード
１７６、３７６、５７６、５７７　エントリ
１８４、３１５、３１６、３１７、５１６、５１７　メッセージサーバ
１８５、５８５　その他のネームサーバ
３１６　メッセージサーバコンピュータシステム
３２８、３５３、５２９、５５３　メッセージ分類モジュール
３３６　許可サーバレコード
３７１、５４５、５７５　電子メッセージ
３７２　ドメイン名

３７５　ネームサービスメッセージ
３７７　ネームサーバ応答
３７９、３７８　許可サーバクエリ
５０８　ネームサーバコンピュータシステム
５１３　ネームサーバ応答
５１４、５７６　ＥＴＰ証明書
５２７、５５２　応答確認モジュール
５２８　パズル計算モジュール
５３７　応答確認サポートレコード
５４１、５４２、５４３　メールクライアント
５４６　メッセージデータ
５４７　応答ドキュメント
５５６　証明書レコード
５８５　ネームサーバメッセージ
５８６　ＥＴＰクエリ

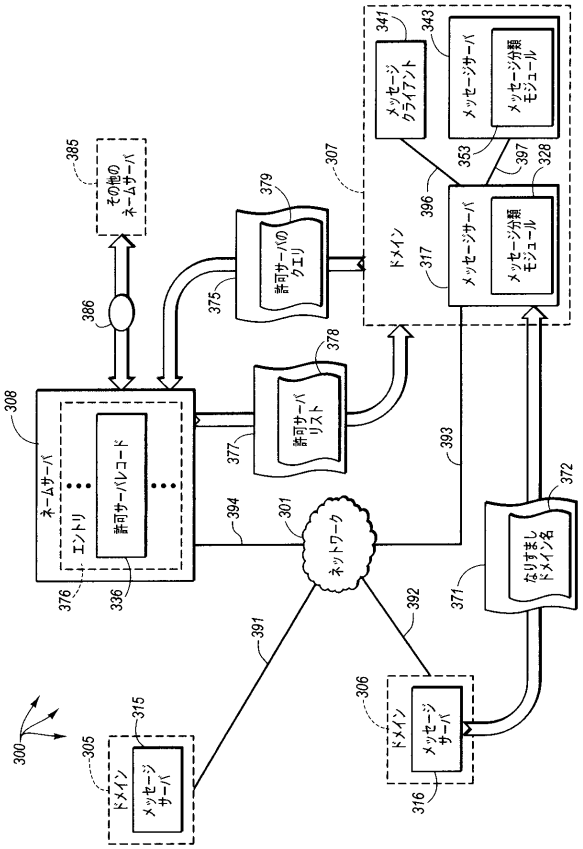
【図１】



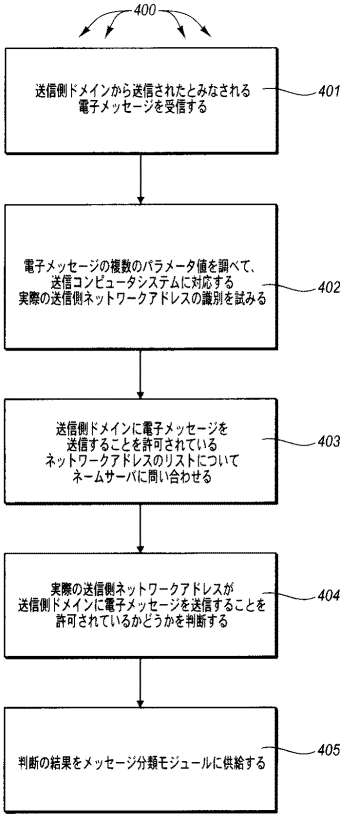
【図２】



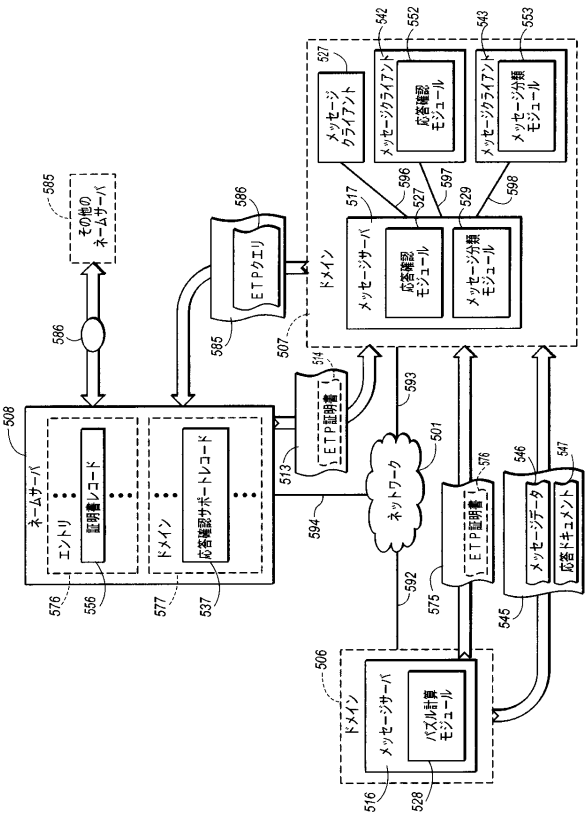
【図３】


その他のネームサーバ
385
386
許可サーバ/Oクエリ
379
375
307
ドメイン
メッセージクライアント
341
メッセージサーバ
343
メッセージ分類モジュール
353
397
328
396
317
メッセージサーバ
メッセージ分類モジュール
許可サーバリスト
378
377
308
ネームサーバ
エントリ
許可サーバレコード
376
336
393
394
301
ネットワーク
372
なりすましドメイン名
371
392
391
306
ドメイン
メッセージサーバ
316
300
315
305
ドメイン
メッセージサーバ

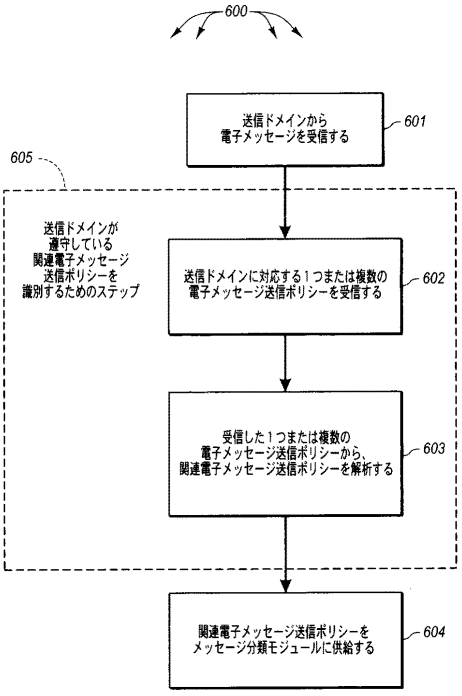
【図４】


400
送信側ドメインから送信されたとみなされる電子メッセージを受信する
401
電子メッセージの複数のパラメータ値を調べて、送信コンピュータシステムに対応する実際の送信側ネットワークアドレスの識別を試みる
402
送信側ドメインに電子メッセージを送信することを許可されているネットワークアドレスのリストについてネームサーバに問い合わせる
403
実際の送信側ネットワークアドレスが送信側ドメインに電子メッセージを送信することを許可されているかどうかを判断する
404
判断の結果をメッセージ分類モジュールに供給する
405

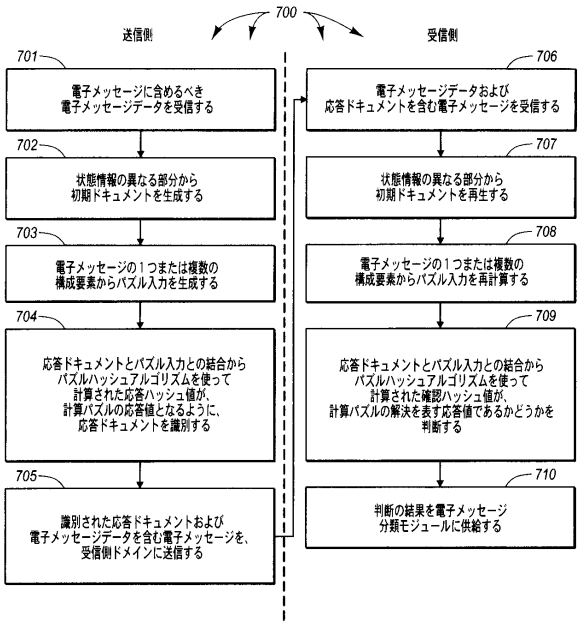
【図５】


その他のネームサーバ
585
586
ETPクエリ
585
586
507
ドメイン
メッセージクライアント
527
応答確認モジュール
542
552
メッセージクライアント
メッセージ分類モジュール
543
553
596
597
598
517
527
529
メッセージサーバ
応答確認モジュール
メッセージ分類モジュール
514
ETP証明書
513
508
ネームサーバ
エントリ
証明書レコード
ドメイン
応答確認サポートレコード
576
556
577
537
593
501
ネットワーク
594
592
575
ETP証明書
546
547
メッセージデータ
応答ドキュメント
545
506
ドメイン
メッセージサーバ
パズル計算モジュール
516
528

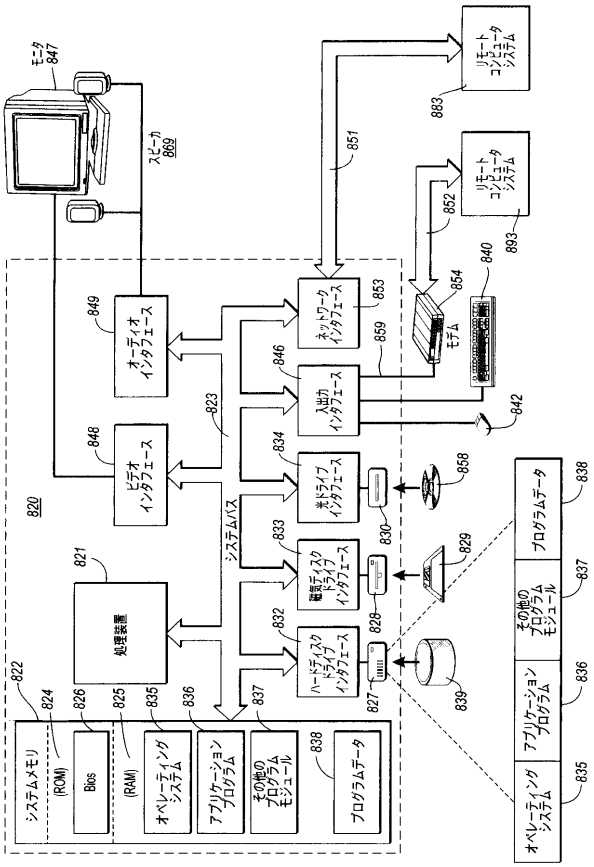
【図６】


600
送信ドメインから電子メッセージを受信する
601
605
送信ドメインが遵守している関連電子メッセージ送信ポリシーを識別するためのステップ
送信ドメインに対応する1つまたは複数の電子メッセージ送信ポリシーを受信する
602
受信した1つまたは複数の電子メッセージ送信ポリシーから、関連電子メッセージ送信ポリシーを解析する
603
関連電子メッセージ送信ポリシーをメッセージ分類モジュールに供給する
604

【図７】


700
送信側
受信側
701
電子メッセージに含めるべき
電子メッセージデータを受信する
702
状態情報の異なる部分から
初期ドキュメントを生成する
703
電子メッセージの１つまたは複数の
構成要素からパズル入力を生成する
704
応答ドキュメントとパズル入力との結合から
パズルハッシュアルゴリズムを使って
計算された応答ハッシュ値が、
計算パズルの応答値となるように、
応答ドキュメントを識別する
705
識別された応答ドキュメントおよび
電子メッセージデータを含む電子メッセージを、
受信側ドメインに送信する
706
電子メッセージデータおよび
応答ドキュメントを含む電子メッセージを受信する
707
状態情報の異なる部分から
初期ドキュメントを再生する
708
電子メッセージの１つまたは複数の
構成要素からパズル入力を再計算する
709
応答ドキュメントとパズル入力との結合から
パズルハッシュアルゴリズムを使って
計算された確認ハッシュ値が、
計算パズルの解決を表す応答値であるかどうかを
判断する
710
判断の結果を電子メッセージ
分類モジュールに供給する

【図８】


モニタ 847
スピーカ 869
リモートコンピュータシステム 883
リモートコンピュータシステム 893
851
852
840
854
モデム
842
ネットワークインタフェース 853
入出力インタフェース 846
859
オーディオインタフェース 849
ビデオインタフェース 848
823
820
システムバス
光ドライブインタフェース 834
磁気ディスクドライブインタフェース 833
ハードディスクドライブインタフェース 832
858
830
829
828
827
839
821
処理装置
822
824
826
825
835
836
837
838
システムメモリ
(ROM)
Bios
(RAM)
オペレーティングシステム
アプリケーションプログラム
その他のプログラムモジュール
プログラムデータ
プログラムデータ 838
その他のプログラムモジュール 837
アプリケーションプログラム 836
オペレーティングシステム 835

フロントページの続き

(72)発明者 ジョシュア ティー. 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
(72)発明者 ジェームズ エム. リオン
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 ４４ コート １６２１７
(72)発明者 ロイ ウィリアムズ
アメリカ合衆国 ９８０７２ ワシントン州 ウッディンビル ノースイースト １６９ プレイス １６５２０
(72)発明者 カジャ イー. アハメド
アメリカ合衆国 ９８００６ ワシントン州 ベルビュー サウスイースト ６３ ストリート １６７７２
(72)発明者 ハリー シモン カッツ
アメリカ合衆国 ９８００８ ワシントン州 ベルビュー １６５ プレイス ノースイースト ３２１５
(72)発明者 ロバート エル. ラウンスウェイト
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
(72)発明者 アンドリュー ブイ. ゴールドバーグ
アメリカ合衆国 ９４０６２ カリフォルニア州 レッドウッド シティ レイクビュー ウェイ ９７８
(72)発明者 シンシア ドワーク
アメリカ合衆国 ９４１１７ カリフォルニア州 サンフランシスコ アッパー テラス ４２５ ナンバー３

審査官 ▲はま▼中 信行

(56)参考文献 特表２００１－５１８７２４（ＪＰ，Ａ）
特開２００２－３３４１６２（ＪＰ，Ａ）
特表２００３－５２６１６４（ＪＰ，Ａ）
特開２００２－３５４０４４（ＪＰ，Ａ）
保坂岳深，外３名，メールフィルタリングシステム，ＮＥＣ技報，日本電気株式会社，２０００年１１月２４日，第53巻，第11号，p.56～59
A DNS RR for simple SMTP sender authentication draft-danisch-dns-rr-smtp-00.txt，２００２年１２月，p.1～6，インターネット<http://tools.ietf.org/html/draft-danisch-dns-rr-smtp-00>

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １３／００
Ｇ０６Ｆ １５／００
Ｈ０４Ｌ １２／５８