(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2012-110032
(P2012-110032A)
(43)公開日　平成24年6月7日(2012.6.7)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/58	(2006.01)	H04L	12/58	100B	5B084
G06F 13/00	(2006.01)	G06F	13/00	610S	5J104
H04L 9/32	(2006.01)	H04L	9/00	675B	5K030
G09C 1/00	(2006.01)	G09C	1/00	640D	

審査請求 有　請求項の数 40　ＯＬ　（全 43 頁）

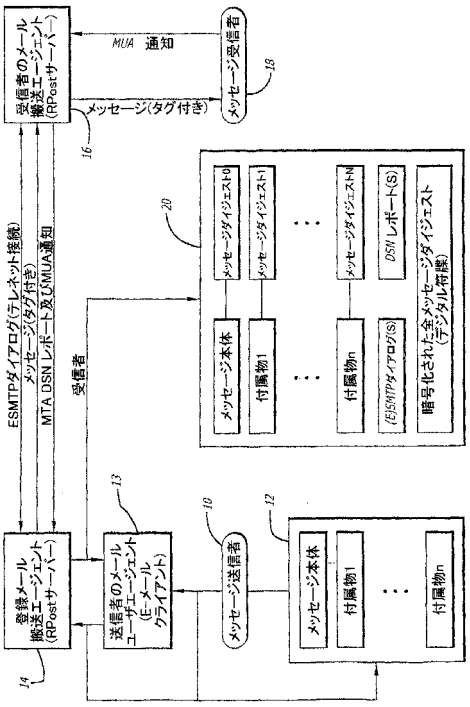
(21)出願番号　特願2012-23225(P2012-23225)
(22)出願日　平成24年2月6日(2012.2.6)
(62)分割の表示　特願2009-42721(P2009-42721)の分割
原出願日　平成13年7月25日(2001.7.25)
(31)優先権主張番号　09/626,577
(32)優先日　平成12年7月27日(2000.7.27)
(33)優先権主張国　米国(US)

(71)出願人　503037631
アールポスト　インターナショナル　リミテッド
アメリカ合衆国　カリフォルニア州　９００４５　ロサンゼルス　ウェスト　センチュリー　ブールヴァード　６０３３　スイート　１２７０
(74)代理人　100059959
弁理士　中村　稔
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】電子メッセージの配達及び完全性を検証するシステム及び方法

(57)【要約】
【課題】ｅ－メールのような電子メッセージの内容及び配達を、機密で且つ偽造防止のドキュメンテーションにより、確実に検証するためのシステム及び方法を提供する。
【解決手段】サーバーは、特定の受信人に送信又は転送されるｅ－メールを受信し、そしてサービスプロバイダーによりメッセージが「登録」されたことを示すためにメッセージに「タグ付け」する。次いで、サーバーは、受信人のメールユーザエージェント（ＭＵＡ）との直接テレネット接続を確立し、そしてタグ付きｅ－メールを受信人のＭＵＡ及び他の受信人のＭＵＡに送信する。メッセージが首尾よく受信されたという受信側ＭＵＡからの応答を受け取った後に、サーバーは、電子受領書を作成してメッセージ発信者へ転送する。
【選択図】図１



【特許請求の範囲】
【請求項１】
送信者から行先アドレスへ、その行先アドレスから転置されたサーバーを経て、メッセージを送信し、そしてそのメッセージを認証する方法であって、
前記サーバーにおいて、
前記送信者から前記メッセージを受信するステップと、
前記メッセージを前記行先アドレスへ送信するステップと、
前記行先アドレスにおいて前記メッセージが受信されたという指示を前記行先アドレスから受信するステップと、
前記メッセージを維持すると共に、更に、前記メッセージのデジタル符牒を与えるステップと、
前記メッセージを認証するよりも前に、前記送信者による記憶のために前記メッセージ及び前記メッセージのデジタル符牒を前記送信者へ送信するステップと、
を備えたことを特徴とする方法。
【請求項２】
前記サーバーにおいて、前記メッセージ及び前記メッセージのデジタル符牒を前記送信者へ送信した後であって且つ前記メッセージを認証する前に、前記メッセージ及び前記メッセージのデジタル符牒を破棄するステップを更に備えた、請求項１に記載の方法。
【請求項３】
前記サーバーにおいて、
前記メッセージを認証する前であるが、前記メッセージを前記行先アドレスへ送信した後に、前記メッセージのコピー及び前記メッセージのデジタル符牒を前記送信者から受信するステップと、
前記メッセージを認証する前に、前記送信者から受信した前記メッセージのコピー及び前記メッセージのデジタル符牒のデジタル指紋を発生するステップと、
前記デジタル指紋をデジタル符牒と比較するステップと、
前記比較の結果に基づいて前記メッセージを認証するステップと、
を更に備えた、請求項２に記載の方法。
【請求項４】
前記サーバーにおいて、
前記送信者の認識と、前記サーバーの認識及びアドレスと、前記受信者の認識及び行先アドレスとを含む付属物を前記サーバーにおいて与えるステップと、
前記付属物を維持すると共に、更に、前記メッセージの認証の前に前記付属物のデジタル指紋を与えるステップと、
前記メッセージの認証の前に、前記送信者が記憶するために、前記付属物及び前記付属物のデジタル指紋を前記サーバーから前記送信者へ送信するステップと、
前記付属物の認証の前に、前記付属物及び前記付属物のデジタル指紋を前記サーバーにおいて破棄するステップと、
を更に備えた、請求項３に記載の方法。
【請求項５】
前記サーバーにおいて、
前記付属物を維持すると共に、更に、前記メッセージ及び前記付属物の認証の前に、前記付属物のデジタル署名を与えるステップと、
前記メッセージ及び前記付属物の認証の前に、前記送信者が記憶するために、前記付属物及び前記付属物のデジタル署名を前記送信者へ送信するステップと、
を更に備えた、請求項４に記載の方法。
【請求項６】
送信者から受信者の行先アドレスへ、その行先アドレスから転置されたサーバーを通して、メッセージを送信し、そしてそのメッセージを認証する方法であって、
前記サーバーにおいて、

前記送信者から前記メッセージを受信するステップと、
前記サーバーと前記行先アドレスとの間にサーバーを含む送信経路を通して、前記メッセージを前記行先アドレスへ送信するするステップと、
前記メッセージの認証の前に、前記サーバーと前記行先アドレスとの間にサーバーを含むメッセージ送信経路の記録を前記サーバーに送信するステップと、
前記メッセージの認証の前に、前記サーバーにおいて前記メッセージを破壊するステップと、
を備えたことを特徴とする方法。
【請求項７】
前記サーバーは、前記メッセージの認証の前に、前記メッセージと、前記サーバーと前記行先アドレスとの間にサーバーを含む前記メッセージ送信経路の記録とを前記送信者から受信し、そして、
前記サーバーは、前記メッセージと、前記サーバーと前記行先アドレスとの間にサーバーを含む前記メッセージ送信経路の記録とに基づいて、前記メッセージを認証する、
請求項６に記載の方法。
【請求項８】
前記行先アドレスは、前記サーバーからメッセージを受信する複数の行先アドレスの１つであり、
前記サーバーが前記複数の行先アドレスへメッセージを送信するときに、前記サーバーは前記複数の行先アドレスの各々を区別し、
前記サーバーと各行先アドレスとの間の前記メッセージ送信経路の記録には、前記サーバーの認識及びアドレスと、前記行先アドレスにおける受信者の認識とが含まれる、
請求項６に記載の方法。
【請求項９】
サーバーにおいてサーバーから行先アドレスへの電子メッセージの配達を与え、そしてその電子メッセージを認証する方法であって、
前記サーバーにおいて、
前記サーバーにより前記行先アドレスへ送信するために送信者からの前記電子メッセージを前記サーバーで受信するステップと、
前記メッセージに関連していて、ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルにより、前記サーバーから前記行先アドレスへ前記電子メッセージを送信し、前記選択されたプロトコルは、前記メッセージに関する前記サーバーと前記行先アドレスとの間の検討と、前記サーバーと前記行先アドレスとの間の前記メッセージ送信経路の記録とを与えるステップと、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記電子メッセージに関する前記サーバーと前記行先アドレスとの間の送信の記録を前記サーバーで受信するステップと、
を備えた方法。
【請求項１０】
前記サーバーにおいて、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記電子メッセージに関する前記サーバーと前記行先アドレスとの間の送信の記録に、前記送信者の認識、前記サーバーの認識及びアドレス、並びに前記行先アドレスを含ませるステップを更に備えた、請求項９に記載の方法。
【請求項１１】
前記サーバーにおいて、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記サーバーと前記送信者との間の前記電子メッセージに関する送信に、前記電子メッセージのデジタル符牒を含ませるステップと、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記サーバーと前記行先アドレスとの間の送信の記録に、前記サーバーから前記行先ア

ドレスへの前記電子メッセージの送信の時間と、前記行先アドレスにおける前記電子メッセージの受信の時間とを記録するステップと、
を更に備えた請求項１０に記載の方法。
【請求項１２】
前記サーバーにおいて、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記サーバーと前記行き先アドレスとの間の前記電子メッセージに関する送信の記録に、前記サーバーから受信者への前記行先アドレスにおける前記電子メッセージの配達の状態を含ませるステップと、
前記行先アドレスにおける前記電子メッセージの配達の状態と、前記行先アドレスから前記受信者への前記電子メッセージの配達とに関する配達状態通知を前記サーバーで受信するステップと、
を更に備えた請求項９に記載の方法。
【請求項１３】
受信者に対する行先サーバーへの電子メッセージの配達を第１サーバーで検証する方法であって、
前記第１サーバーにおいて、
前記メッセージの認証の前に、前記メッセージに関連していて、ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルにより、前記第１サーバーから前記行先サーバーへ前記電子メッセージを送信するステップと、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記電子メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信を、前記行先サーバーから前記第１サーバーで受信するステップと、
前記メッセージの認証の前に、前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録とを、前記第１サーバーから前記送信者へ送信するステップと、
を備えた方法。
【請求項１４】
前記メッセージの認証の前に、前記第１サーバーにおいて、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の完了時間に前記電子メッセージを前記第１サーバーから前記送信者へ送信するステップと、
前記メッセージの認証の前に、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記電子メッセージに関する前記送信が前記第１サーバーにより前記送信者へなされた後に、前記第１サーバーにおいて前記電子メッセージを破棄するステップと、
を備えた請求項１３に記載の方法。
【請求項１５】
前記第１サーバーにおいて、
前記電子メッセージを前記第１サーバーに維持すると共に、更に、前記メッセージの認証の前に、前記電子メッセージのデジタル符牒を前記第１サーバーにおいて与えるステップと、
前記メッセージの認証の前に、前記第１サーバーから前記送信者へ前記電子メッセージを送信する時間に、前記第１サーバーから前記送信者へ前記電子メッセージのデジタル符牒を送信するステップと、
を更に備えた請求項１３に記載の方法。
【請求項１６】
前記第１サーバーにおいて、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の後であって、前記メッセージの認

証の前に、前記電子メッセージを前記第１サーバーから前記送信者へ送信するステップと、
　前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記電子メッセージに関する前記送信が前記第１サーバーにより前記送信者へなされた後であるが、前記メッセージの認証の前に、前記第１サーバーにおいて前記電子メッセージを破棄するステップと、
を更に備えた請求項１５に記載の方法。
【請求項１７】
　前記第１サーバーと前記行先サーバーとの間に、前記送信者の認識、前記第１サーバーの認識及びアドレス、前記行先サーバーの認識及びアドレス、前記第１サーバーによる前記電子メッセージの受信の時間、並びに前記行先サーバーから前記第１サーバーへ前記送信者の認識、前記第１サーバーの認識及びアドレス、及び前記行先サーバーの認識及びアドレスを送信する時間を送信ステップと、
　前記第１サーバーから前記行先サーバーへの前記電子メッセージの配達の状態を指示する配達状態通知と、前記行先サーバーにより前記第１サーバーへ前記配達状態通知を送信する時間とを、前記行先サーバーから前記第１サーバーで受信するステップと、
を更に備えた請求項１３に記載の方法。
【請求項１８】
　前記第１サーバーで、前記第１サーバー及び前記行先サーバーの中間のサーバー間での送信を含む付属物を与え、
　前記第１サーバーから前記送信者へ電子メッセージを送信することは、前記付属物を送信することを含み、
　前記第１サーバーからのメッセージは、前記第１サーバーが、前記メッセージ及び付属物の認証の前に、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録を含めて、前記電子メッセージ及び付属物を前記送信者へ送信するときに廃棄される、請求項１５に記載の方法。
【請求項１９】
　前記第１サーバーにおいて、
　ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルによる前記メッセージに関連した、前記送信者の認識、前記第１サーバーの認識及びアドレス、並びに前記行先サーバーの認識及びアドレスの送信を、前記行先サーバーから前記第１サーバーで受信するステップと、
　ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルによる前記メッセージ及びメッセージに関する情報の前記第１サーバーから前記送信者への送信ときに、前記送信者の認識、前記第１サーバーの認識及びアドレス、並びに前記行先サーバーの認識及びアドレスを前記第１サーバーから前記送信者へ送信するステップと、
　前記メッセージの認証の前に前記電子メッセージを破棄するステップと、
を備えた請求項１７に記載の方法。
【請求項２０】
　前記第１サーバーにおいて、前記メッセージの認証の前に、
　前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つのプロトコルによる前記送信者からの前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録を含めて、前記電子メッセージのデジタル署名を前記第１サーバーにおいて与えるステップと、
　前記メッセージと、前記メッセージの前記デジタル署名とを前記第１サーバーから前記送信者へ送信するステップと、
を備えた請求項１６に記載の方法。
【請求項２１】

受信者に対する行先サーバーへの電子メッセージの配達を第１サーバーで検証する方法であって、前記第１サーバーにおいて、
前記電子メッセージを前記行先サーバーへ送信するためにメッセージ送信者からの前記電子メッセージを前記第１サーバーで受信するステップと、
ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルにより、前記電子メッセージ及びそのメッセージに関連した情報を前記第１サーバーから前記行先サーバー送信するステップと、
前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信を前記第１サーバーで受信するステップと、
前記メッセージの認証の前に前記電子メッセージを、そして前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録の少なくとも特定の部分を、前記第１サーバーから前記送信者へ送信するステップと、
を備えた方法。
【請求項２２】
前記送信者への前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する送信の記録の少なくとも特定の部分とは、前記メッセージの認証の前に、前記送信者により前記第１サーバーへ与えられ、そして
前記電子メッセージは、前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記送信者から第１サーバーへの送信の記録の少なくとも特定の部分とに基づいて前記第１サーバーにより認証される、請求項２１に記載の方法。
【請求項２３】
前記電子メッセージは、前記第１サーバーに位置され、そして更に、前記第１サーバーにおいて前記電子メッセージのデジタル署名が与えられ、
前記デジタル署名は、前記メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録の少なくとも特定の部分と共に、前記第１サーバーから前記送信者へ送信され、そして
前記デジタル署名は、その後、前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記送信の記録の少なくとも特定の部分と共に、前記メッセージの認証の前に、前記送信者により前記第１サーバーへ与えられる、請求項２１に記載の方法。
【請求項２４】
前記電子メッセージのデジタル符牒と、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つにより与えられるメッセージに関する電子送信のデジタル符牒とが前記第１サーバーに発生されて、前記メッセージの認証の前に、前記送信者へ送信され、
前記デジタル符牒と、前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記送信の少なくとも特定の部分が、その後、前記メッセージの認証の前に、前記送信者により前記第１サーバーへ与えられ、
前記第１サーバーにおいて前記メッセージからデジタル指紋が生成され、そして、前記電子メッセージのデジタル符牒が当該メッセージの認証の前に、前記送信者により前記第１サーバーへ与えられ、そして
前記電子メッセージは、前記第１サーバーにおいて発生されるデジタル指紋と前記デジタル符牒の間で認識を確立することにより前記第１サーバーにおいて認証される、請求項２２に記載の方法。
【請求項２５】
第１サーバーから行先サーバーへの電子メッセージの配達を第１サーバーにおいて検証する方法であって、

前記第１サーバーにおいて、
前記行先サーバーへ送信するためにメッセージ送信者からの前記電子メッセージを前記第１サーバーで受信するステップと、
前記第１サーバーから前記行先サーバーへ前記電子メッセージを送信するステップと、
ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の電子的送信を前記第１サーバーで受信するステップと、
前記メッセージの認証の前に、前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の前記電子的送信の記録とを、前記第１サーバーから前記送信者へ送信するステップと、
前記メッセージの認証の前に、前記電子メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の前記電子的送信の記録とを、前記送信者から前記第１サーバーで受信するステップと、
前記第１サーバーにより前記送信者から受信した前記電子メッセージと、前記第１サーバーにより前記送信者から受信した前記電子的送信の記録とに基づいて、前記第１サーバーにおいて前記電子メッセージを認証するステップと、
を備えた方法。
【請求項２６】
前記第１サーバーにおいて、
前記メッセージの認証の前に、前記サーバーから前記送信者へ送信される電子的情報を前記送信者から前記サーバーへ送信するステップと、
前記送信者から前記サーバーへ送信された情報に基づいて前記電子メッセージを認証するステップと、
を備えた請求項２５に記載の方法。
【請求項２７】
前記第１サーバーにおいて、
前記電子メッセージを維持すると共に、更に、前記電子メッセージのデジタル符牒を与え、又、電子的付属物を維持すると共に、更に、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の前記電子的送信の記録を含むものである電子的付属物のデジタル符牒を与えるステップと、
前記メッセージの認証の前に、前記電子メッセージ及び前記電子的付属物が前記サーバーから前記送信者へ送信されるのと同時に、前記電子メッセージのデジタル符牒及び前記電子的付属物のデジタル符牒を前記サーバーから前記送信者へ送信するステップと、
を備えた請求項２６に記載の方法。
【請求項２８】
前記第１サーバーにおいて、
前記電子メッセージを維持すると共に、更に、前記電子メッセージのデジタル署名を与え、又、前記電子的付属物を維持すると共に、更に、前記電子的付属物のデジタル署名を与えるステップと、
前記メッセージの認証の前に、前記電子メッセージ及び電子的付属物と、前記電子メッセージ及び電子的付属物のデジタル署名とを、前記第１サーバーから前記送信者へ送信するステップと、
を備えた請求項２６に記載の方法。
【請求項２９】
送信者により与えられ、そして送信者及び行先サーバーから転置された第２サーバーにより行先サーバーへ送信される付属物を認証する方法であって、前記第２サーバーにおいて、

前記付属物の認証の前に、前記付属物に関するＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つにより前記第２サーバーと前記行先サーバーとの間に送信される前記電子的付属物を与えるステップと、
前記付属物の認証の前に、前記電子的付属物を前記第２サーバーから前記送信者へ送信するステップと、
を備えた方法。
【請求項３０】
前記第２サーバーにおいて、
前記電子的付属物を維持すると共に、更に、前記電子的付属物の認証の前に、前記第２サーバーにおいて前記電子的付属物のデジタル符牒を与えるステップと、
前記付属物の認証の前に、前記電子的付属物を前記第２サーバーから前記送信者へ送信するときに、前記電子的付属物のデジタル符牒を前記第２サーバーから前記送信者へ送信するステップと、
前記電子的付属物及び前記電子的付属物のデジタル符牒を、前記送信者へ送信した後であるがそれらの認証の前に、前記第２サーバーにおいて破壊するステップと、
前記電子的付属物及び前記電子的付属物のデジタル符牒を、前記付属物の認証の前に、前記送信者から前記第２サーバーで受信するステップと、
前記第２サーバーにより前記送信者から受信された前記電子的付属物及び前記電子的付属物のデジタル符牒に基づいて、前記第２サーバーにおいて前記電子的付属物を認証するステップと、
を更に備えた請求項２９に記載の方法。
【請求項３１】
前記第２サーバーにおいて、
前記付属物の認証の前に、前記送信者から前記第２サーバーで前記電子的付属物及び前記電子的付属物のデジタル符牒を受信するステップと、
前記付属物の認証の前に、前記送信者から前記第２サーバーで受信された前記電子的付属物のデジタル指紋及び前記電子的付属物のデジタル符牒を前記第２サーバーにおいて与えるステップと、
前記デジタル指紋を比較して、前記電子的付属物を認証するステップと、
を更に備えた請求項３０に記載の方法。
【請求項３２】
送信者により与えられ、そして送信者及び行先サーバーから転置された第２サーバーにより行先サーバーへ送信されるメッセージを認証する方法であって、　前記第２サーバーにおいて、
前記送信者の認識及びアドレスと、前記第２サーバーの認識及びアドレスと、前記行き先サーバーの認識及びアドレスとを含む電子的付属物を与えるステップと、
前記第２サーバーから前記行先サーバーへメッセージを送信した後であって、前記第２サーバーによる前記電子的付属物の認証の前に、前記第２サーバーから前記送信者へ前記電子的付属物を送信するステップと、
前記電子的付属物を前記送信者へ送信した後であって、前記電子的付属物の認証の前に、前記第２サーバーにおいて前記電子的付属物を破棄するステップと、
を備えた方法。
【請求項３３】
前記付属物の認証の前に前記第２サーバーから前記送信者へ前記電子的付属物が送信され、前記電子的付属物は、前記第２サーバーと前記行先サーバーとの間の前記電子的付属物の送信において前記電子的付属物を受信する中間ステーションのアドレス及び認識を含む、請求項３２に記載の方法。
【請求項３４】
前記第２サーバーにおいて、
前記電子的付属物を維持すると共に、更に、前記メッセージの認証の前に、前記第２サ

ーバーにおいて前記付属物のデジタル符牒を与えるステップと、
前記メッセージの認証の前に、前記電子的付属物を前記第２サーバーから前記送信者へ送信するときに、前記電子的付属物のデジタル符牒を前記第２サーバーから前記送信者へ送信するステップと、
前記電子的付属物及び前記電子的付属物のデジタル符牒を、前記メッセージの認証の前に、前記送信者から前記第２サーバーで受信するステップと、
前記メッセージの認証の前に、前記第２サーバーにより前記送信者から受信された前記電子的付属物及び前記電子的付属物のデジタル符牒に基づいて、前記第２サーバーにおいて前記電子的付属物を認証するステップと、
を更に備えた請求項３３に記載の方法。
【請求項３５】
前記第２サーバーにおいて、
前記付属物の認証の前に、前記送信者からの前記付属物及び前記付属物のデジタル署名を前記第２サーバーで受信するステップと、
前記付属物の認証の前に、前記送信者から前記第２サーバーで受信された前記付属物のデジタル署名及び前記付属物のデジタル指紋を前記第２サーバーにおいて与えるステップと、
前記第２サーバーにおいて前記デジタル指紋を比較して、前記付属物を認証するステップと、
を更に備えた請求項３３に記載の方法。
【請求項３６】
電子メッセージ、及び行先アドレスへの電子メッセージの配達をサーバーにおいて認証する方法であって、
前記サーバーにおいて、
前記サーバーと行先アドレスとの間で電子メッセージを送信するステップと、
前記サーバーと行先アドレスとの間のメッセージ送信経路であって、前記サーバーと行先アドレスとの間のサーバーを含むような経路の記録を前記サーバーで受信するステップと、
前記メッセージの認証の前に、前記電子メッセージ、及び前記サーバーと行先アドレスとの間の電子メッセージ送信経路の記録を前記送信者へ送信するステップと、
を備えた方法。
【請求項３７】
前記サーバーは、前記メッセージ、及び前記サーバーと行先アドレスとの間のメッセージ送信経路の記録を前記送信者へ送信した後であって、前記メッセージの認証の前には、前記メッセージも、前記サーバーと行先アドレスとの間のメッセージ送信経路の記録も保持しない、請求項３６に記載の方法。
【請求項３８】
前記サーバーは、前記メッセージの認証の前に、前記メッセージ、及び前記サーバーと行先アドレスとの間のメッセージ送信経路の記録を前記送信者から受信し、
前記サーバーは、前記メッセージの認証の前に、前記メッセージ、及び前記サーバーと行先アドレスとの間のメッセージ送信経路の記録を前記サーバーにより前記送信者から受信するのに基づいて、前記メッセージを認証する、請求項３６に記載の方法。
【請求項３９】
前記サーバーは、メッセージを維持すると共に、更に、メッセージのデジタル署名を与え、そしてメッセージの認証の前に、このデジタル署名をメッセージと共に前記送信者へ送信し、
前記サーバーは、メッセージの認証の前に、メッセージ及びメッセージのデジタル署名を前記送信者から受け取り、そして
前記サーバーは、メッセージのデジタル指紋及びメッセージのデジタル署名を与え、そしてデジタル指紋を前記デジタル符牒と比較して、メッセージを認証する、請求項３６に

記載の方法。
【請求項４０】
第１サーバーにより送信者から受信されそして第１サーバーにより受信者のための行先サーバーへ送信されるメッセージを第１サーバーにおいて検証する方法であって、
前記第１サーバーにおいて、
前記メッセージの認証の前に、前記送信者からのメッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録を含む付属物を前記行先サーバーから前記第１サーバーで受信し、前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信は、ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルより成るグループから選択されたプロトコルにより与えられ、
前記メッセージの認証の前に、前記メッセージと、前記ＳＭＴＰプロトコル及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記第１サーバーと前記行先サーバーとの間の送信の記録を含む前記付属物とを前記第１サーバーから前記送信者へ送信し、
前記メッセージの認証の前に、前記メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記送信の記録を含む前記付属物とを前記送信者から前記第１サーバーへ送信し、そして
前記第１サーバーにより前記送信者から受信された前記メッセージと、前記ＳＭＴＰ及びＥＳＭＴＰプロトコルの選択された１つによる前記メッセージに関する前記送信の記録を含む前記付属物とに基づいて、前記メッセージを認証する、
というステップを備えた方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的に、電子メッセージの配達及び内容を検証するシステム及び方法に係り、より詳細には、ｅ－メールメッセージの配達及び内容に関する証明を後で与えるシステム及び方法に係る。
【背景技術】
【０００２】
近年、ｅ－メールは、必須のビジネスツールになった。ｅ－メールは、速く、安くそして一般的により信頼性が高いので、多くの業務慣習の「蝸牛郵便」に取って代わっている。しかしながら、書留郵便や配達証明郵便のようなハードコピーが依然主流であるような幾つかのメールアプリケーションが残されている。例えば、手紙が配達証明郵便で配達されるときには、その手紙が郵送されたことを証明する受領書が差出人に与えられる。返送される書留郵便の受領書は、受信人又は受信人が許可した代理人に手紙が首尾よく配達されたという郵便業務の確認を付加する。更に、Ｆｅｄｅｒａｌ　Ｅｘｐｒｅｓｓ（登録商標）及びＵｎｉｔｅｄ　Ｐａｒｃｅｌ　Ｓｅｒｖｉｃｅ（登録商標）（ＵＰＳ）のような民間のクーリエは、ある形式の配達確認を与える。クーリエ郵便は、実際上、一通ごとに登録されるので、顧客は、配達証明を希望するときには、それらのサービス利用に転じることは当然である。
【０００３】
多くの既存のｅ－メールシステムやｅ－メールプログラムは、ある形式の配達証明を既に与えている。例えば、あるｅ－メールシステムでは、今日、送信者がメッセージに「通知要求」タグをマークすることができる。このようなタグは、メッセージが配達されたこと及び／又はメッセージをいつオープンしたかの通知を送信者が要求できるようにする。送信者が配達通知を要求するときには、インターネットのｅ－メールシステムは、メッセージが受信者のメールサーバー又は電子インボックスに配達されたというｅ－メール受領書を送信者に与える。この受領書メッセージは、メッセージのタイトルと、行先アドレスと、配達時刻とを含む。又、このメッセージは、（メーリングソフトウェアに設けられてアクチベートされる「フラグ」の形式に基づいて）メッセージがその行先への途中に通過

する全てのインターネット「ステーション」のリストも含む。この形式のレポートは、ｅ－メールを実施するルール及びプロトコルの幾つかに組み込まれる。更に、メッセージが「読み取り通知」要求と共に送信されるときには、受信者のｅ－メールプログラムは、受信者がそのメッセージを読むためにオープンしたというｅ－メール通知を送信者へ送信する。多くの電子メールクライアントは、この種のレポートをサポートできそしてサポートするが、インターネットプロトコルは、この命令を行うものではない。

【０００４】

しかしながら、これは、通知要求と共に送信されるｅ－メールが全ての観点において書留郵便と同じ有効性であることを意味しない。人々が手紙を配達証明や書留にするのは、配達の証拠、例えば、民事又は刑事訴訟に使用できる証拠、或いはメッセージが送信され、ジョブが完了され、注文が出され、又は契約要件が満足したことで監督者、クライアント又は政府機関を満足させる証拠を希望するからである。

【０００５】

米国ポスタルサービス（ＵＳＰＳ）からの書留受領書は、ＵＳＰＳが後援することにより配達証明を構成する。この受領書は、当該手紙や荷物がその住所又は許可された代表者に実際に配達されたという郵便局の確認を表わす。他方、ｅ－メール受領書の場合には、ｅ－メールが、法廷においてメッセージが配達された証拠としての説得力のある証拠品として受け入れられ信頼されるには、種々のハードルが存在する。結局、この受領書は、誰かがいつでも変更したり又は作成したりすることのできる単なる別のｅ－メールメッセージかもしれない。

【０００６】

ｅ－メールによる通信の便宜性及び低コスト性の利点を充分に取り入れるために、ｅ－メールメッセージの内容及び配達の信頼性ある証拠を与えることのできるｅ－メールシステム及び／又は方法が要望されている。

この要望を満足するために、サービス中に記録することにより送信者が第三者の配達証明を受け取ることのできる幾つかのシステムが確立されている。

ａ）送信者は、電子メッセージを、文書の意図された受信者のリストと共に第三者に送信する。

ｂ）第三者は、メッセージの意図された受信者の各々に通知を送信して、そのメッセージを見ることのできる第三者のウェブサイトを訪れるように招待する。

ｃ）意図された受信者が第三者のウェブサイトを訪れてそのメッセージを見た場合には、第三者がその訪問を記録し、従って、送信者は、自分のメッセージを受信者が読んだことを知ることができる。

【０００７】

このようなシステムの欠点は種々様々ある。第１に、それらシステムは、本質的に、ｅ－メールの受信者が協力して第三者のサービスからそれらのメッセージを収集することに依存している。しかしながら、送信者がメッセージの配達証明を希望する環境は、意図された受信者が協力してメッセージを受信すると仮定できない場合がしばしばある。例えば、メッセージの確認受領書が受信者に財政的又は法的な負担を課する場合には、受信者は、メールを受信できるという通知を単に無視することができる。このようなシステムでは、意図された受信者が待機中メールの通知を受信したことを保証するものは何もないことに注意されたい。第２に、このようなシステムは、各メッセージを送信し、収集しそしてその配達を検証するために送信者及び／又は受信者がワールドワイドウェブサイトに接続することを必要とするので、通常のｅ－メールに比して、使用が厄介で且つ低速である。更に、このような方法による文書の送信は、送信者及び受信者の両方がウェブサイトにファイルをアップロード及びダウンロードすることを必要とする。最後に、これらの方法は、メッセージが収集されるか又は時間切れとなるときまで第三者が各メッセージの全コピーを保持する必要があるので、そのプロバイダーが、実質的な計算リソースを長時間にわたってデータ記憶及びデータ追跡に捧げることを必要とする。配達証明を与える別の方法として、あるシステムは、受信者が同じｅ－メールクライアントを使用するならば、メッ

セージが受信されたときに送信者に通知する独占的ｅ－メールクライアント又はウェブブラウザプラグインを与える。このようなシステムは、送信者及び受信者の両方が同じｅ－メールクライアントを使用する必要があるという明らかな欠点がある。

【０００８】

それ故、電子メッセージの内容及び配達について信頼性のある証拠を与えることができ、受信者の承諾又は協力を必要とせず、送信者又は受信者の側に特殊なｅ－メールソフトウェアを必要とせず、従来のｅ－メールと同じ又はほぼ同じ便宜性及び使用速度で動作し、そしてサービスプロバイダーによって経済的に動作することのできるｅ－メールシステム／方法の必要性が存在する。

【発明の概要】

【課題を解決するための手段】

【０００９】

本発明の一般的な目的は、ｅ－メールのような電子メッセージの内容及び配達を、機密で且つ偽造防止のドキュメンテーションにより、確実に検証するためのシステム及び方法を提供する。理想的には、本発明は、米国の書留郵便より優れていなくてもそれと同等の法的状態をｅ－メール及び他の電子メッセージに与える。しかしながら、本発明は有用な情報及び検証を与えるものであるから、ここに教示する方法に基づいて送信されるメッセージに対し何らかの特定の法的状態が容認されることは本発明にとって必要のないことである。

【００１０】

本発明は、システムを経て送信される各電子メッセージのデジタル符牒を形成しそして記録する電子メッセージシステムを包含する。発信者は、電子メッセージのコピーをシステムに送信するか、又はシステム自体の中で電子メッセージを発生する。次いで、システムは、電子メッセージを、「ｔｏ（主宛先）」アドレス及び「ｃｃ（コピー配布先）」アドレスを含む全ての受信者に（又は受信者に関連した行先メッセージハンドラーに）転送及び配達する。その後に、システムは、配達受領書を電子メッセージの発信者に返送する。この受領書は、とりわけ、オリジナルメッセージと、メッセージのデジタル符牒と、受信者への配達時刻を含むハンドシェーク及び配達経過とを含む。受領書に含まれた情報を後で検証及び認証するために、発信者即ちユーザは、受領書のコピーをシステムに送信する。システムは、次いで、デジタル符牒がオリジナルメッセージ及び受領書の他部分に一致することを検証する。両者が一致する場合には、システムは、手紙を送信するか、又は電子メッセージが変更されていないことを検証する他の認証確認を与える。

【００１１】

システムは、インターネットに接続されたｅ－メールサーバーの形態でよく、これは、多数のやり方で使用することができる。例えば、個々のユーザは、システムへ「カーボンコピー」（ｃｃ：）を送信するか又はシステム自体の中でメッセージを構成することにより、ｅ－メールのような電子メッセージを登録することができる。会社又はｅ－コマースユーザの場合に、それらユーザは、そのサーバーを本発明によるサーバーに対して変更し、そしてそれらの全外部電子メッセージを登録することができ、更に、システムが受領書を保持しそして公的記録するというオプションをもつことができる。システムは、暗号化された電子メッセージを受け入れて検証し、そして「ファイアウオール」内及び／又は外で電子メッセージを管理することができる。ウェブベースのユーザ、即ちＭＳＮ　Ｈｏｔｍａｉｌ（登録商標）やＹａｈｏｏ　Ｍａｉｌ（登録商標）のようなウェブベースのｅ－メールを使用する個人又は会社の場合に、それらユーザは、ボックスをチェックするか、さもなければ、それらのｅ－メールプログラム内のフラグをセットし、ｅ－メールを登録すべきかどうか及び／又は本発明のシステムを使用してメッセージを公的記録すべきかどうかケース・バイ・ケースで選択することができる。

【００１２】

デジタル符牒は、既知のデジタル符牒技術を使用して形成することができ、例えば、メッセージに対してハッシュ関数を遂行してメッセージのダイジェストを形成しそしてその

メッセージのダイジェストを暗号化することにより形成することができる。メッセージの本体、付属物、本体及び付属物を含む全メッセージ、そして個々のメッセージダイジェストに対して、個別のデジタル符牒を形成することができる。暗号化されたメッセージダイジェストは、ある形式のメッセージ認証又は有効確認コード、或いは機密ドキュメンテーションを与える。他のメッセージ認証及び／又は有効確認コードを発生しそして使用することもできる。

【００１３】

１つの特徴において、本発明は、電子メッセージの配達及び内容に関する証拠を与える方法において、送信者からコンピュータネットワークを横切って電子メッセージを受け取り、このメッセージは、それに関連した配達アドレスを有し、このメッセージに基づいてメッセージダイジェストを計算し、このメッセージダイジェストを暗号化し、上記配達アドレスに対応する行先にメッセージを電子的に送信し、メッセージの配達に作用する「簡単なメール搬送プロトコル（ＳＭＴＰ）」又は「拡張型ＳＭＴＰ（ＥＳＭＴＰ）」ダイアログを記録し、上記メッセージ及び配達アドレスに関連した「配達状態通知」情報を受け取り、上記送信者に電子受領書を与え、この受領書は、メッセージのコピーと、暗号化されたメッセージダイジェストと、（Ｅ）ＳＭＴＰトランスクリプトと、「配達状態通知」情報の少なくともサブセットとを含むものであり、そして将来の期日に、送信者から上記電子受領書を電子的に受信し、上記暗号化されたメッセージダイジェストが上記メッセージに対応することを検証し、そして上記メッセージが、上記配達アドレスに関連した電子メッセージハンドラーにより受信されたことを検証するという段階を備えた方法を提供する。

【００１４】

別の特徴において、本発明は、電子メッセージの配達を検証する方法において、ワイドエリアネットワークコンピュータシステム内で、行先アドレスへルーティングするためにメッセージ送信者から電子メッセージを受信し、行先アドレスに関連した電子メッセージサーバーとの通信を確立し、該サーバーは、行先サーバーを形成し、この行先サーバーに質問して、該行先サーバーが「配達状態通知（ＤＳＮ）」機能をサポートするかどうか決定し、その質問に対する応答を受信し、その質問及び応答は一緒にＳＭＴＰダイアログを形成し、このＳＭＴＰダイアログの結果に基づいて行先サーバーから「配達状態通知」情報を要求し、上記電子メッセージを行先アドレスへ送信し、上記電子メッセージの配達に対して上記行先サーバーからＤＳＮ情報を受信し、そして上記ＳＭＴＰダイアログの少なくとも一部分及び上記ＤＳＮ情報の少なくとも一部分を上記メッセージ送信者に与えるという段階を備えた方法を提供する。

【００１５】

更に別の特徴において、本発明は、受信した電子メッセージの内容を検証する方法において、電子メッセージを受信し、その受信したメッセージの内容に対応するデジタル符牒を発生し、上記メッセージ及びデジタル符牒を行先アドレスに与え、そしてその後、上記デジタル符牒が上記メッセージに対応することを検証するという段階を備えた方法を提供する。

【００１６】

本発明の更に別の特徴によれば、上記方法は、メッセージが受信者により電子的に受信されたかどうか確立することを含むもので、送信者から受信者のアドレスと共に電子的に発送されるべきメッセージを用意し、このメッセージに関連した符牒を形成し、そのメッセージを受信者のアドレスへ電子的に発送し、そのメッセージを追跡して、受信者のアドレスへ発送されたメッセージの最終的な「配達状態」を決定し、このメッセージの最終的な「配達状態」を受信すると、受領書を発生し、該受領書は、メッセージのコピーと、符牒と、メッセージの最終的な「配達状態」とを含むものであり、そしてその受領書を送信者に与えて、メッセージが受信者により電子的に受信されたことを後で確立するという段階を備えている。

【００１７】

本発明の更に別の特徴によれば、受信者に送信された電子メッセージが読み取られたことを証明するための方法において、電子メッセージを受信者のアドレスと共に与え、その電子メッセージに対応するデジタル符牒を計算し、その電子メッセージを受信者のアドレスに電子的に発送し、受信者から「メールユーザエージェント（ｅ－メールクライアント「読み取り」）通知を要求し、その読み取り通知を受信した際に、読み取り受領書を発生し、この読み取り受領書は、メッセージのコピーと、対応電子メッセージに対するデジタル符牒と、受信者からの読み取り受領書に対する第２のデジタル符牒とを含むものであり、そして上記メッセージが受信者により受信されたことを後で検証するためにこの読み取り受領書を与えるという段階を備えた方法が提供される。

【００１８】

本発明の更に別の特徴によれば、電子メッセージのコピーとされているものの完全性を確認するための方法において、上記電子メッセージのコピーとされているものを受信し、このコピーとされているものは、それに関連した暗号化されたメッセージダイジェストを含み、このメッセージダイジェストを暗号解読し、上記コピーとされているものの内容に基づいて第２のメッセージダイジェストを発生し、そして上記暗号解読されたメッセージダイジェストと上記第２のメッセージダイジェストとを比較して２つのメッセージダイジェストが一致するかどうか決定することにより上記コピーとされているものを有効性確認するという段階を備えた方法が提供される。

【００１９】

本発明の更に別の特徴によれば、受信された登録ｅ－メールを有効確認するための方法において、電子的な受領書を受け取り、該受領書は、ベースメッセージ及び暗号化されたメッセージダイジェストを含むものであり、更に、その暗号化されたメッセージダイジェストを暗号解読し、上記ベースメッセージから第２メッセージダイジェストを発生し、そして上記暗号解読されたメッセージダイジェストが上記第２メッセージダイジェストに一致する場合に上記ｅ－メールを有効とする段階を備えた方法が提供される。

【００２０】

更に別の特徴において、本発明は、ユーザが機密メッセージを送信及び受信するために行くことのできるウェブサイトであって、ウェブサイトのホストが独立した第三者として働いて、メッセージを送信及び受信すると共に、メッセージの内容及び配達に関して機密のドキュメンテーションを与えるようなウェブサイトに係る。

本発明の上述した目的、並びに本発明の他の特徴及び効果は、同じ部分が同じ番号で示された添付図面を参照した好ましい実施形態の以下の詳細な説明、及び特許請求の範囲から当業者に容易に明らかとなろう。

【図面の簡単な説明】

【００２１】

【図１】出て行くメッセージが特殊な「メール搬送エージェント（ＭＴＡ）」により送信されることによって登録される本発明の第１実施形態を示すシステム図である。

【図２Ａ】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャートである。

【図２Ｂ－１】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャートである。

【図２Ｂ－２】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャートである。

【図２Ｃ】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャートである。

【図２Ｄ】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャートである。

【図２Ｅ】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャートである。

【図２Ｆ】図１の実施形態に基づき出て行くｅ－メールを登録するためのフローチャート

である。
【図３】送信者が個別の登録ＭＴＡを経て選択されたメッセージを送信するように「メール搬送エージェント」に指令できる本発明の第２実施形態を示すシステム図である。
【図４】出て行くメッセージのカーボンコピー（ｃｃ）が、登録されるべき特殊なサーバーへ送信される本発明の第３実施形態を示すシステム図である。
【図５】ユーザが、行先ウェブサイトに登録されるべき出て行くメッセージを構成する本発明の第４実施形態のシステム図である。
【図６】ユーザが、「ウェブベースのメールユーザエージェント（ＭＵＡ）」内から登録されたｅ－メールを送信しそして受領書を記憶する本発明の第５実施形態のシステム図である。
【図７ａ】登録されたｅ－メール受領書を有効確認するフローチャートである。
【図７ｂ】登録されたｅ－メール受領書を有効確認するフローチャートである。
【図８】到来するメッセージを登録するための本発明の実施形態のシステム図である。
【図９】到来するメッセージを登録するためのフローチャートである。
【図１０】受け取った登録メッセージを有効確認するためのフローチャートである。
【図１１】到来する及び出て行く通信を登録しそして確認するためにｅ－ビジネスにより本発明を使用する一例を示すシステム図である。
【発明を実施するための形態】
【００２２】
以下、添付図面を参照して、本発明の好ましい実施形態を詳細に説明する。
この説明は、何ら限定を意図するものではなく、本発明の一般的な原理を単に例示するものに過ぎない。以下の詳細な説明の章の表題及び全体的な編成は便宜的なものに過ぎず、本発明を限定するものではない。従って、本発明は、インターネットネットワークアーキテクチャー及びインフラストラクチャーを使用するｅ－メールメッセージシステムに関して説明する。ここに説明する特定のメッセージ形式及びネットワークアーキテクチャーは、説明上のものに過ぎず、本発明は、布線及び無線ネットワークを含む他のコンピュータネットワークアーキテクチャーを使用する他の電子メッセージプロトコル及びメッセージ形式にも適用できる。説明の便宜上、本発明によって処理されるメッセージは、ここでは「登録（書留）」メッセージと称する。以下の説明において、「ＲＰｏｓｔ」という語は、一般に、本発明を実施するソフトウェア及び／又はハードウェアを形成し及び／又は動作し、及び／又は指定の第三者メッセージ検証者として働く第三者エンティティを指すものとする。この語は、例示の便宜上使用されるものに過ぎず、本発明を限定するものではないと理解されたい。
【００２３】
Ｉ．出メールサーバーとしてのＲＰｏｓｔの実施形態
図１は、出て行くｅ－メールが本発明により登録される本発明の第１実施形態のシステム図である。この実施形態において、ＲＰｏｓｔ登録サーバー１４は、メッセージ送信者のメールユーザエージェント（ＭＵＡ）１３に対する一次の出メール搬送エージェント（ＭＴＡ）として働く。メッセージ受信者１８は、技術的には、受信人であり、それ故、この時点では、単に意図された受信者又は意図された行先であるが、説明を簡略化するため、このエンティティは、ここでは、受信者、受信人又は行先と称する。単一のメッセージが多数の異なる行先を有してもよく、そしてそれらの各々に異なるＭＴＡを経て到達できることに注意されたい。
【００２４】
登録メッセージを送信する方法は、次の３つの部分に分割することができる。
１）前処理：メッセージを送信する前に行われるステップ；
２）送信：メッセージを受信人に配達する方法；
３）後処理：配達、受領書の作成及び受領書の有効確認の後にメッセージに関する情報を収集するための手順。
【００２５】

１．１　前処理

送信のためのメッセージを受け取ると、ＲＰｏｓｔサーバーは、各メッセージに対してデータベースに記録を形成し、これは、次のような情報を記憶するのに使用される。

ａ）メッセージが受信された時刻

ｂ）メッセージの付属物の名前

ｃ）メッセージのアドレスの番号

【００２６】

メッセージの行先ごとに、データベースは、次のものを記録する。

ａ）行先の名前（もし得られれば）

ｂ）行先のインターネットアドレス

ｃ）メッセージが行先のメールサーバーに配達された時刻

ｄ）この行先の配達状態

システムにより使用される受信者の配達状態は、次のものを含む。

ＵＮＳＥＮＴ（非送信）

この状態は、メッセージが送信されなかったことを示す。

ＤＥＬＩＶＥＲＥＤ－ＡＮＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）

この状態は、成功／失敗通知を予想できるように配達状態通知（ＤＳＮ）をサポートするＥＳＭＴＰ適合ＭＴＡへメッセージが配達されたことを示す。

【００２７】

ＤＥＬＩＶＥＲＥＤ（配達済み）

この状態は、この受信者に送信されたメッセージのコピーが、ＥＳＭＴＰ　ＤＳＮをサポートしないサーバーへ首尾良く配達されたことを意味する。

ＤＥＬＩＶＥＲＥＤ－ＴＯ－ＭＡＩＬＢＯＸ（メールボックスへ配達済み）

この状態は、この受信者へ送信されたメッセージのコピーが受信者のメールボックスへ配達されたことを示すＤＳＮメッセージが受け取られたことを意味する。

ＲＥＬＡＹＥＤ（中継済み）

この状態は、この受信者へ送信されたメッセージのコピーが別のサーバーへ更に中継されたことを示すＭＴＡ　ＤＳＮが受け取られたことを意味する。

ＵＮＤＥＬＩＶＥＲＡＢＬＥ（配達不能）

この状態は、試みを繰り返した後に、ＲＰｏｓｔがこの受信者へメッセージを配達するためにＭＴＡに接続できなかったことを示す。

ＦＡＩＬＥＤ（失敗）

この状態は、この受信者へのメッセージのコピーの配達が失敗であったことを示すＭＴＡ　ＤＳＮが受け取られたことを意味する。

【００２８】

このとき、システムは、メッセージの内容に対してハッシュ関数も実行する。

ＲＰｏｓｔサーバー１４は、ハッシュ関数及び暗号アルゴリズムを使用する。ハッシュ関数は、ＭＤ２、ＭＤ５又は機密ハッシングアルゴリズム（ＳＨＡ）を含む良く知られたハッシュ関数の１つ、或いは将来開発されるであろう他のハッシュ関数でもよい。ハッシュアルゴリズム及び方法は、１９９３年、ジョン・ウィリー＆ソンズ・インク（ニューヨーク）、ブルース・シュナイダー著の「Applied Cryptography: Protocols, Algorithms, and Source Code in C」；フェデラル・インフォーメーション・プロセッシング・スタンダード・パブリケーション１８０－１（ＦＩＰＳ　ＰＵＢ１８０－１）「Secure Hash Standard」、ナショナル・インスティテュート・オブ・スタンダーズ・アンド・テクノロジー；及びクラウクジク氏の「Distributed Fingerprints for Information Integrity Verification」と題する米国特許第５，５３０，７５７号に記載されており、これらは、ハッシュ関数、暗号化、並びにそれら関数を実施するための方法及びシステムの教示について参考としてここに援用するものである。メッセージの内容が変更されたかどうか検出する他の既知の又は新規な方法が使用されてもよい。

【００２９】
良好なハッシュ関数Ｈは、一方向性であり、即ち逆転が困難である。ここで、「逆転が困難」とは、あるハッシュ値ｈが与えられたときに、Ｈ（ｘ）＝ｈというようにある入力ｘを見出すことが計算上不可能であることを意味する。更に、ハッシュ関数は、少なくとも弱く無衝突でなければならず、これは、あるメッセージｘが与えられたときに、Ｈ（ｘ）＝Ｈ（ｙ）というようにある入力ｙを見出すことが計算上不可能であることを意味する。その結果、使用するアルゴリズム及びそれにより生じるハッシュ値又はメッセージダイジェストを知っている自称捏造者でも、同じ番号にハッシュする偽造メッセージを形成することができない。ハッシュ関数により返送されるハッシュ値ｈは、一般に、メッセージダイジェストと称される。このメッシュダイジェストは、メッセージｘの「デジタル指紋(fingerprint)」とも称される。現在、一方向性のハッシュ関数は、結果が安全で、捏造されないことを確保するために、少なくとも１２８ビット長さの出力を発生することが推奨される。現在の技術状態が進歩するにつれて、安全ハッシュ関数として推奨される長さが増加するであろう。

【００３０】
ＲＰｏｓｔサーバー１４は、メッセージ本体に対するメッセージダイジェストと、メッセージの各付属物に対する個別のメッセージダイジェストとを計算し、そしてそれらを、メッセージの受領書に後で含ませるように記憶する。
登録に必要なようにメッセージを変更する前に、オリジナルメッセージ及びその付属物のコピーは、それらを後でシステムによって検索できるように記憶される。
ＲＰｏｓｔサーバーは、メッセージを、受信者のＭＴＡへ送信する前に多数のやり方で変更することができる。

【００３１】
本発明の実施にとって必要ではないが、メッセージが登録されたことを表わすためにメッセージにタグを付けることができ、これは、例えば、メッセージの「当該」ラインの始めに「登録済み」という語を挿入するか、又は「このメッセージは、ＲＰｏｓｔに登録されている。付加的な情報については、当方のウェブサイトｗｗｗ．ＲＰｏｓｔ．ｃｏｍへおいで下さい」というタグをオリジナルメッセージの終わりに添付するか、或いは他のタグにより行われる。更に、タグは、インストラクションや、ワールドワイドウェブアドレスや、リンクを含んでもよく、これは、登録メッセージを構成して送信できるウェブページにリンクすることにより受信者を招待してそのメッセージに対して登録応答を送信できるようにする。
タグは任意であるが、配達されたメッセージは、ここでは、一般に、タグ付きメッセージと称する。
インターネットプロトコルは、ｅ－メールメッセージに対して２つの形式の受領書を与える。

【００３２】
ＭＴＡ通知
これは、種々の事象が生じたというメッセージの名目送信者を表わす受信者のＭＴＡにより送信されるｅ－メールである。ＳＭＴＰプロトコルに合致するＭＴＡは、通常、差出人が受信人のメールボックスにメッセージを配達できない場合にのみ通知を送信する（これは、アドレスが有効でないか、又は受信人のメールボックスがその割り当てられた記憶量を越えた場合に生じる）。

【００３３】
拡張ＳＭＴＰ規格が導入されると、送信側ＭＴＡがメッセージ配達の成功及び失敗の通知を要求できるようになった。この配達状態通知（ＤＳＮ）は、ある事象が生じたとき、例えば、メッセージが受信者のメールボックスに首尾良く入れられたとき、何らかの理由で受信者のメールボックスにメッセージを配達できないとき、又はＤＳＮ受領書を与えない別のサーバーへ受信者のメッセージが中継されたときに、受信側ＭＴＡによりメッセージの名目送信者に送信されるｅ－メールである。

【００３４】
拡張ＳＭＴＰ（ＥＳＭＴＰ）プロトコルをサポートするｅ－メールサーバーのみがこの形式のＤＳＮをサポートし、そしてこの機能のサポートは、ＥＳＭＴＰサーバーにとって任意であり、サーバーの管理者により選択されたコンフィギュレーションに依存する。
ＤＳＮは、ＥＳＭＴＰが出現してから使用される用語であるが、以下の説明では、ＥＳＭＴＰプロトコルに適合するかどうかに関わらず受信メッセージの状態に関するＭＴＡ発生メッセージを指すものとして「ＤＳＮ」を使用する。
【００３５】
ＭＵＡ通知（読み取り通知）
これは、ある事象が生じたとき、例えば、メッセージが読み取りのためにオープンされるか、又は読み取られずにシステムから削除されたときに、受信者のメールユーザエージェント（ＭＵＡ）（ｅ－メールプログラム）によりメッセージの（名目上の）著者へ送信されるｅ－メールである。インターネットの規定（ＲＦＣ１８９１）によれば、ＭＵＡプログラムが強制的にこのような通知を発生することはできない。ＭＵＡがこれら受領書を発生するかどうかは、ユーザにより選択されたコンフィギュレーションに依存する。
【００３６】
ＲＰｏｓｔサーバー１４は、適合するＭＴＡ及びＭＵＡからＭＴＡＤＳＮ及びＭＵＡ通知の両方を選択するよう試みるやり方でメッセージを構成しそして送信する。適合するＭＵＡから読み取り受領書を選択するために、ｅ－メールメッセージのヘッダ区分にあるヘッダを含ませねばならない。異なるＭＵＡが異なるヘッダに応答し、従って、サーバー１４は、種々のＭＵＡにより確認される形態で読み取り通知を要求する各メッセージに多数の異なるヘッダを追加する。これらのヘッダは、全て、次の形態をとる。
ヘッダラベル：ユーザ名＜ユーザアドレス＞
例えば、
破棄通知、宛先：ジョン・スミス＜ｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍ＞ 読取通知、宛先：ジョン・スミス＜ｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍ＞ここで、「ジョン・スミス」は、ＭＵＡ通知を送付すべきユーザの名前であり、そして「＜ｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍ＞」は、ユーザのインターネットアドレスである。通常、このようなヘッダは、メッセージの著者を指すが、本発明の方法の場合には、ＲＰｏｓｔにより通知を処理できるように通知をＲＰｏｓｔへ返送することが要求される。これを確実に行うために、サーバー１４は、ＲＰｏｓｔサーバーにより処理を行えるアドレス、例えば、「ｒｅａｄｒｅｃｅｉｐｔ@ＲＰｏｓｔ．ｃｏｍ」へＭＵＡ受領書を送信することを要求するヘッダを挿入する。これは、適合する受信者ＭＵＡに、それらの通知を処理のためにＲＰｏｓｔアドレスに送信するよう命令する。
【００３７】
返送されるＭＵＡ通知を処理するタスクは、この段階で処理しなければならない別の問題を発生する。ＭＵＡ通知のフォーマット又は内容を支配する規格はない。しばしば、それらは、オリジナルメッセージの主題と、事象（例えば、「読み取りのためにオープンする」）の時刻とを引用して、報告する。しかし、たとえこの情報が通知に含まれても、それを促すメッセージを独特に識別するか又はそのメッセージの著者を識別するのに充分であることは稀である。システムは、ＭＵＡ通知を受信すると、それを促すメッセージを識別して、ＲＰｏｓｔが送信者のために発生する受領書に通知情報を含ませることができねばならない。或いは、システムは、少なくとも、ＭＵＡ通知が指すメッセージの送信者を確実に識別して、その通知情報をＲＰｏｓｔ読み取り受領書（以下に述べる）の形態で送信者へ送付できるようにしなければならない。
【００３８】
この後者の目標を達成するために、システムは、インターネットアドレスが、２つの成分、即ち名前フィールド及びアドレスフィールドを有することの利点を取り入れることができ、アドレスフィールドは、コーナー引用符「＜＞」により区切られている。ほとんどのＭＵＡは、それらのＭＵＡ通知の行先アドレスに両フィールドを含む。ＭＵＡ受領書に

対してその要求を構成する際に、ＲＰｏｓｔシステムは、サーバー１４の読み取り受領書取り扱いアドレスを通知のためのアドレスとして含ませるが、ヘッダの名前フィールドにオリジナル送信者のアドレスを使用する。例えば、メッセージのオリジナル送信者が、ユーザであるジョン・スミスで、インターネットアドレスｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍを有する場合には、ＲＰｏｓｔサーバーは、次の形態のヘッダを含む。

破棄通知、宛先：ｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍ ＜ｒｅａｄｒｅｃｅｉｐｔｓ@ＲＰｏｓｔ．ｃｏｍ＞

これは、通常、適合ＭＵＡが、次のようにアドレスされたｒｅａｄｒｅｃｅｉｐｔｓ@ＲＰｏｓｔ．ｃｏｍへ通知を送信する結果となる。

ｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍ ＜ｒｅａｄｒｅｃｅｉｐｔｓ@ＲＰｏｓｔ．ｃｏｍ＞

アドレス「ｒｅａｄｒｅｃｅｉｐｔｓ@ＲＰｏｓｔ．ｃｏｍ」においてこのような通知を受信すると、サーバーは、受信人のフィールドをパージングすることにより、その通知がｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍにより最初に送信されたメッセージに関するものであると決定できる。これは、通知の内容を検査することにより決定できない場合にもそうである。この情報が手元にある状態では、サーバーは、通知の内容をデジタル符牒のＲＰｏｓｔ読み取り受領書で包んで、その受領書をアドレスｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍに送信することができる。

【００３９】

又、ＲＰｏｓｔシステムは、受信者ＭＴＡによって発生されたＭＴＡ　ＤＳＮ通知を選択して収集するようにも努力する。このような通知は、常に、メッセージヘッダの「ＦＲＯＭ（から）：」フィールドにリストされたアドレスへ送られるので、サーバー１４は、メッセージが、ＤＳＮを処理できるＲＰｏｓｔアドレスに「から：」として受け取られるように、各メッセージヘッダを変更しなければならない。

【００４０】

しかしながら、ＤＳＮを処理する問題は、この段階で処理しなければならない別の問題を引き起こす。ＤＳＮは、標準的な内容又はフォーマットを有しておらず、即ちこれらｅ－メールの内容を検査するだけでは、それらの内容がどんなメッセージの通知を与えるか決定することがしばしば不可能となる。この問題は、ＤＳＮ封筒ＩＤ番号を使用することによりＥＳＭＴＰプロトコルに従って発生されたＤＳＮに向けられたものであると仮定する（ＲＦＣ１８６９を参照）。このプロトコルに基づき、送信側ＭＴＡは、ＤＳＮに対する要求と共に参照番号を含ませることができる。この番号は、返送ＤＳＮに引用され、送信者がＤＳＮの当該メッセージを識別できるようにする。しかしながら、実際に、自分自身をサポート側ＥＳＭＴＰ　ＤＳＮとして報告する多くのＭＴＡは、ＤＳＮ封筒ＩＤも、当該メッセージを確実に識別するに充分な他の情報も返送しない。最終的に、あるＤＳＮが、それが通知を与えるところのメッセージを識別するに充分な情報を返送する場合でも、その通知を促したメッセージの特定アドレスを識別するに充分な情報を含まないことがしばしばある。従って、単一のメッセージがドメインにおける２つの受信人に送信され、その一方は、受信人のメールボックスに首尾良く配達され、他方は、配達されない。ドメインに対するＭＴＡは、どの受信人に首尾良く配達されそしてどの受信人には配達されなかったかをＤＳＮの受信者が決定できないようなやり方でこれら事象をＤＳＮにおいて報告する（例えば、ＤＳＮが、受信者のアドレスを、オリジナルメッセージに含まれたアドレスではなくそれらのローカルエイリアス名として報告する場合に起こり得る）。

【００４１】

本発明は、この問題を次の４つの段階で解決する。

１）各々の出て行くメッセージに対し独特の識別番号が発生される（例えば、タイムスタンプに基づいて）。この番号は、データベースに記憶される。

２）各メッセージの受信者は列挙され、そして識別番号がデータベースに記憶される。

３）メッセージは、意図された各受信者のＭＴＡに別々に送信される。（２人の受信者が共通のドメイン名及びＭＴＡを有するときでも、サーバー１４は、２つの別々のＳＭＴ

Ｐテレネットセッションにおいてそのｍｔａへメッセージを送信する）。
４）サーバー１４は、受信者のＭＴＡにメッセージを送信すると、メッセージの「から」フィールドを増大し、メッセージの独特のＩＤ及び送信者の識別番号を組み込んだアドレスから送信されたものとしてメッセージを示す。アドレスは、サーバーが返送メッセージをＤＳＮとして識別できるようにするサブストリング（例えば、「ｒｃｐｔ」）も含む。

【００４２】
従って、ジョン・スミスという名前の送信者からサーバー１４により「ｍｍｙｙｄｄｓｓ」と呼称される単一のメッセージは、次のようなヘッダ表示で第１の意図された受信者（システムにより「ａ」と呼称される）へ送信される。
から：ジョン・スミス＜ｒｃｐｔｍｍｄｄｙｙｓｓａ@Ｒｐｏｓｔ．ｃｏｍ＞同じメッセージが、次のヘッダ表示で第２の受信者へ送信される。
から：ジョン・スミス＜ｒｃｐｔｍｍｄｄｙｙｓｓｂ@Ｒｐｏｓｔ．ｃｏｍ＞多くのｅ－メールＭＵＡは、メッセージの送信者の名前のみを表示し、従って、特殊なアドレスは、ほとんどの受信者から見えない。

【００４３】
この形態のアドレッシングの要旨は、受信者ＭＴＡがＤＳＮを発生するときには（ＥＳＭＴＰに適合するかどうかに関わらず）、ＤＳＮを異なるＲＰｏｓｔアドレスにアドレスする。これらのＤＳＮを受信すると、サーバー１４は、それらを「ＲＣＰＴ」プレフィックスによりＤＳＮメッセージとして識別し、そしてアドレスをパージングすることにより、どのメッセージ及びどの受信者がＤＳＮの対象であるか決定することができる。
システム１４は、メッセージを受信者のＭＴＡへ送信するよう試みるたびにメッセージの受信者を指すように各メッセージの「から」フィールドを変更する。

【００４４】
送信されたメッセージに対する受信者の応答が適切に向けられるように確保するために、システム１４は、オリジナル送信者の名前及びインターネットアドレスを列挙するメッセージに明確な「ｒｅｐｌｙ－ｔｏ（応答宛先）：」メッセージヘッダを追加する。ここに示す例の場合には、これは、次の通りである。
応答宛先：ジョン・スミス＜ｊｓｍｉｔｈ@ａｄｏｍａｉｎ．ｃｏｍ＞
これは、受信者ＭＵＡが、受信メッセージに対する応答を、構成されたＲＰｏｓｔアドレスではなく、実際の送信者のアドレスに向けるように導く。

【００４５】
１．２　送信
上述したように、方法の一部分として、ＲＰｏｓｔサーバーは、出て行くメッセージの個別のコピーをそのメッセージの各受信人へ送信する。更に、ＲＰｏｓｔは、各行先に対し記録のメール交換機（ＭＸ）で直接的なＳＭＴＰ接続を経て各々の配達を行うように試みる。
注：各有効なインターネットｅ－メールアドレスは、インターネットドメイン名又はＩＰアドレスを含む。各ドメイン名／アドレスには、そのドメイン内のアドレスに対してメールを受信することが許されたｅ－メールサーバー（１つ又は複数）が関連される。あるドメインは、２つ以上のサーバーを有することに注意されたい。各ドメインを担当するドメイン名サーバーは、インターネットを横切ってそのメールサーバーの認識をブロードキャストする。この情報は、公衆に利用できるもので、インターネットｅ－メール及びドメイン名サーバーを支配するルール及び規定に合致するやり方で管理されそして送信される。

【００４６】
メッセージのコピーを行先へ送信する前に、ＲＰｏｓｔサーバーは、行先のドメインに関連したＭＴＡを識別するためにインターネット名サーバールックアップを実行する。行先アドレスに代わってメールを受信する役割を果たすＭＴＡを識別すると、システムは、行先のローカルＭＴＡとのテレネット接続をオープンするように試みる。

インターネットｅ－メールを、それらが最終的な行先に到達するまでＭＴＡからＭＴＡへ中継するのが一般的な慣習である。ＲＰｏｓｔサーバーと行先ＭＴＡとの間に直接的な接続を要求する主たる目的は、ＲＰｏｓｔサーバーが、受信者ドメイン名に対するｅ－メールを受信する独占的役割を果たすｅ－メールサーバーと共に、メッセージの配達を記録できるようにすることである（この記録は、ＳＭＴＰダイアログの形態をとる）。

【００４７】

この記録の存在は、書留郵便の受領書が配達の証拠を与えるのと良く似た方法で、メッセージが配達された有用な証拠を与える。ＵＳＰＳ書留郵便は、受信人の許可された代理人（例えば、秘書又はメールルームの事務員）に配達されたことを証明できる場合に、検証可能に配達されるものとして処理される。ＲＰｏｓｔ配達受領書の証拠としてのメリットに対して法的に挑戦する場合には、インターネットのｅ－メールサービスプロバイダーを選択する際に、そのプロバイダーが受信者に代わり電子メッセージを収集することを受信者が許可することが確認される。次いで、そのサービスプロバイダーは、そのＭＴＡのアドレスをこのドメインに対する受け入れｅ－メールサーバーとしてブロードキャストすることにより、そのドメイン名のｅ－メール受信者の許可されたエージェントとしてその状態を確認する。

【００４８】

従って、受信者のｅ－メールを受信する役割を果たすメールサーバーへメッセージを直接配達すると、ＲＰｏｓｔは、受信者が自分のメールを受信するために法的に許可したエージェントへメッセージを配達する。配達トランザクション（このトランザクションは、ＳＭＴＰダイアログの形態をとる）を記録することにより、ＲＰｏｓｔは、受信者の許可したエージェントへの配達の証拠を得るように請求することができる。

【００４９】

ここに述べる方法は、各行先への配達の他の形式の証拠を収集するように試みるが、それらの試みが成功するか否かは、ＲＰｏｓｔの制御には存在しないファクタ（例えば、受信者のメールサーバーに配備されるＳＭＴＰサポートの形式）に依存することに注意されたい。他方、受信者のメールサーバーへの配達指令が成功するたびに、常に、ＳＭＴＰ記録が発生される。この記録を記録すると、ＲＰｏｓｔは、インターネットメールに対する最小プロトコル（ＳＭＴＰ）に適合する有効なインターネット行先への配達の証拠を与えることができる。これは、ＥＳＭＴＰ　ＤＳＮに依存することにより配達を証明するよう試みる他の方法に勝る現在の方法の重要な効果を表わす。

【００５０】

メッセージの行先に対してＭＴＡを識別すると、ＲＰｏｓｔサーバーは、ＲＦＣ１８６９に合致する「ＥＨＬＯ」ハンドシェークを発生することによって行先ＭＴＡとのＥＳＭＴＰ接続をオープンするように試みる。サーバー１６がＥＳＭＴＰをサポートする場合には、それがどのＥＳＭＴＰサービスをサポートするかリストすることにより応答する。

サーバー１６がＥＳＭＴＰをサポートする場合には、ＲＰｏｓｔサーバーは、先ず、サーバー１６がＥＳＭＴＰサービス「ＶＥＲＩＦＹ（検証）」をサポートするかどうか決定する。この検証サービスは、発呼ＳＭＴＰサーバーが、とりわけ、ＭＴＡドメインのアドレスが本物であるかどうか決定できるようにする。ＲＰｏｓｔサーバーが、これらの手段により、そのメッセージを配達しようと試みているアドレスが有効でないと決定する場合には、接続を終了し、このアドレスへのメッセージ配達の試みを停止し、そしてこのメッセージ行先の状態を「ＵＮＤＥＬＩＶＥＲＡＢＬＥ（配達不能）」としてそのデータベースに記録する。

【００５１】

その結果に関わらず、ＲＰｏｓｔサーバーは、ＥＳＭＴＰ　ＶＥＲＩＦＹダイアログをファイルに記録すると共に、それを、そのメッセージの配達受領書に後で付属させるか又は含ませることができるように記憶する。セキュリティとの関連性から、若干のＥＳＭＴＰサーバーがＶＥＲＩＦＹファンクションをサポートすることに注意しなければならない。

システム１６がＶＥＲＩＦＹ方法をサポートしない場合にも、ＲＰｏｓｔサーバーは、システム１６へメッセージを配達するよう試みる。通常、ＭＴＡは、名目上そのドメイン内にあるアドレスに対するメッセージを受け入れ、そしてそのアドレスが無効である場合にＤＳＮを後で送信する。

【００５２】

次いで、ＲＰｏｓｔサーバーは、行先サーバーがＥＳＭＴＰサーバーＤＳＮをサポートするかどうか決定するよう試みる。もしそうであれば、ＲＰｏｓｔは、受信人への配達が成功又は失敗した場合に、ＥＳＭＴＰ　ＤＳＮでメッセージの送信者にサーバー１６が通知するという要求と共にメッセージを送信する。この行先へのメッセージの送信が成功した後に、システムは、この行先の配達状態を「ＤＥＬＩＶＥＲＥＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）」として記録する。

【００５３】

サーバー１６が、ＥＳＭＴＰをサポートしないことを指示するように「ＥＨＬＯ」ハンドシェークに応答する場合には、ＲＰｏｓｔサーバーは、ＳＭＴＰ接続を開始するために「ＨＥＬＯ」メッセージを発生する。この接続が達成される場合には、ＲＰｏｓｔサーバーは、ＳＭＴＰプロトコルに適合するようにメッセージを送信し、そして行先の配達状態を「ＤＥＬＩＶＥＲＥＤ（配達済み）」として記録する。

【００５４】

接続がＳＭＴＰであるかＥＳＭＴＰであるかに関わらず、ＲＰｏｓｔサーバーは、２つのサーバー間の全プロトコルダイアログを記録する。通常、このダイアログは、プロトコルメッセージを含み、とりわけ、行先サーバーは、それ自身を識別し、名前のある受信者に対してメッセージをアップロードするための許可を与え、そしてメッセージが受け取られたことを確認する。ＲＰｏｓｔは、このトランザクションの記録をセーブして、それが後で検索されそしてこのメッセージに対するＲＰｏｓｔ配達受領書に含まれ又は付属されるようにする。

【００５５】

種々の理由で、ＲＰｏｓｔは、受信者のＭＴＡとのＳＭＴＰ接続を達成できないことがあり、又はこのような接続は得られるが受信者によりメッセージを送信する許可が拒絶されることがある。この場合、インターネットＤＮＳルックアップが、行先アドレスが多数のＭＴＡによりサービスされることを表わすならば、ＲＰｏｓｔサーバーは、それらの各々にそのメッセージを配達するよう試みる。ＲＰｏｓｔは、システムリソースが許す頻繁さで適当なＭＴＡに配達を試み続ける。ある長さの時間の後に、ＲＰｏｓｔがメッセージをアドレスに配達できない場合には、このメッセージのこの受信者の状態を「ＵＮＤＥＬＩＶＥＲＡＢＬＥ（配達不能）」とマークし、そしてこのメッセージをこの行先アドレスに送信する試みを停止する。

【００５６】

ＲＰｏｓｔサーバーは、ＥＳＭＴＰ　ＤＳＮを明確にサポートする行先サーバーへメッセージを首尾良く送信するときには、このメッセージに対するこの受信者の状態を「ＤＥＬＩＶＥＲＥＤ－ＡＮＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）」として記録する。

ＲＰｏｓｔサーバーは、ＥＳＭＴＰ　ＤＳＮを明確にサポートしない接続を経て行先サーバーへメッセージを首尾良く送信するときには、このメッセージに対するこの受信者の状態を「ＤＥＬＩＶＥＲＥＤ（配達済み）」として記録する。

【００５７】

１．３　後処理

ＤＳＮ処理

ＭＴＡ　ＤＳＮは、独占的ドメイン（例えば、「ＲＰｏｓｔ．ｃｏｍ」）の架空のアドレスにアドレスされたＲＰｏｓｔサーバーへ返送され、これらのアドレスは、上述したように構成される。ＲＰｏｓｔサーバーは、そのドメインにアドレスされた全てのインバウンドメールを走査し、そしてそれらの識別サブストリング（例えば、「ｒｃｐｔ」）によ

りＤＳＮメッセージを検出する。これらアドレスを上述したようにパージングすることにより、システムは、メッセージと、ＤＳＮ通知を促した受信者とを識別することができる。

【００５８】

ＤＳＮメッセージに対する標準的なフォーマットはなく、又、それらの結果を報告する標準的な語彙もない。受信したＤＳＮを評価するために、システムは、主題ライン及びＤＳＮメッセージの本体を、ＤＳＮの意味を表わすワード及びフレーズについて見なければならない。例えば、「首尾良い配達」又は「メールボックスへ配達された」又は「配達された」というフレーズは、通常、ＤＳＮに関するメッセージが行先のメールボックスに入れられたことを表わす。システムは、このようなフレーズを検出すると、メッセージのこの行先の配達状態を「ＤＥＬＩＶＥＲＥＤ　ＴＯ　ＭＡＩＬＢＯＸ（メールボックスへ配達された）」に変更する。

【００５９】

「配達できなかった」、「致命的エラー」、「失敗」及び「不首尾な」というフレーズは、通常、メッセージを行先へ配達するためのＭＴＡによる失敗を報告するＤＳＮを表わす。ＤＳＮにおいてこれらのフレーズを検出すると、システムは、受信者の配達状態の記録を「失敗」に変更する。

システムは、常に、行先のドメインに対して独占的ＭＴＡへメールを配達するが、これらのＭＴＡは、時には、メッセージを異なるサーバーへ中継する（例えば、受信側ＭＴＡがファイアウオールの後方にメールを送信するような場合に）。この場合に、ＤＳＮは、「中継された」又は「前方に中継された」等のフレーズを含む。この場合、システムは、受信者の配達状態を「ＲＥＬＡＹＥＤ（中継された）」に変更する。

ＤＳＮを評価しそしてそれに応じて受信者の配達状態を更新すると、システムは、それが含むＤＳＮ及び付属物をセーブし、このメッセージ（１つ又は複数）がＲＰｏｓｔ配達受領書に含まれ及び／又は付属されるようにする。

【００６０】

メッセージの管理

時々、システムは、各送信メッセージを走査し、そしてそのメッセージの各行先の状態を検査して、システムがその行先の配達の処理を完了したかどうか決定する。完了に対する基準は、行先の配達状態に基づく。

ＤＥＬＩＶＥＲＥＤ（配達済み）：この状態は、この受信者のメッセージのコピーが、ＥＳＭＴＰ　ＤＳＮをサポートしないＭＴＡに配達されたことを指示する。それでも、このようなＭＴＡは、受信人のメールボックスにメッセージを配達できない場合に（例えば、行先アドレスがドメイン内の有効口座に対応しない場合に起こり得る）、ある形式の配達状態通知を送信することができる。従って、システムは、受信者ＭＴＡへの配達以来、ある時間周期が経過するまで、このような受信者に対する配達を完了として処理しない。この時間周期（通常、２ないし２４時間）は、大多数のサーバーが配達失敗通知を返送するに必要な最大時間の推定値を表わし、これは、特定の行先ドメインが離れているか、或いはこのような通知を発生するのが早いか又は遅いことが分かっている場合に調整される。

【００６１】

ＲＥＬＡＹＥＤ（中継済み）：この状態は、ＥＳＭＴＰ　ＤＳＮをサポートしない別のＭＴＡへ受信者ＭＴＡがメッセージを転送したことを指示するＤＳＮが受け取られたことを意味する。この場合、それでも、メッセージが配達されたＭＴＡが、やがて、配達失敗通知を送信することが考えられる。従って、この状態を伴う受信者は、状態ＤＥＬＩＶＥＲＥＤ（配達済み）を伴う受信者と同じ条件のもとで完了として処理される。

【００６２】

ＤＥＬＩＶＥＲＥＤ－ＡＮＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）：この状態は、受信者のＭＴＡがＥＳＭＴＰ　ＤＳＮをサポートし、そしてＤＳＮが懇請されるがまだ受け取られていないことを示す。ＭＴＡは、それ自身、この

サービスをサポートするものとして識別するが、それでも、首尾良い配達の場合に、ＤＳＮを与えないことが時々起こり得る。従って、システムは、ある時間インターバルの後にＤＳＮが受信されない場合でも、この状態を伴う行先への配達を完了とみなす。このインターバル（通常、６ないし２４時間）は、適合するＭＴＡがＤＳＮを返送するのに通常要求される最大時間の推定値を表わす。

【００６３】

ＤＥＬＩＶＥＲＥＤ－ＴＯ－ＭＡＩＬＢＯＸ（メールボックスへ配達済み）：この状態は、首尾良い配達を示すＤＳＮがこの受信者に対して受け取られ、従って、この行先へのメッセージの配達が完了したことを指示する。

ＦＡＩＬＥＤ、ＵＮＤＥＬＩＶＥＲＡＢＬＥ（失敗、配達不能）：この状態を伴う受信者への配達は、常に、完了として処理される。

メッセージの全受信者への配達が完了したことがシステムに分かると、システムは、メッセージに対する配達受領書を構成する。

【００６４】

配達受領書の形成

配達受領書は、登録メッセージのオリジナル送信者へ送信されるｅ－メールである。受領書２０は、次のものを含む。

１．管理のための識別子。この識別子は、送信者ＩＤに対するリファレンス、及び／又はシステムにより受信された送信者のメッセージのインターネットメッセージＩＤの値であってもよいし又はそれを含んでもよい。

２．受領書が発生された日付及び時刻。

３．オリジナルメッセージの引用された本体と、その意図された受信者のｅ－メールアドレス。

４．ＲＰｏｓｔサーバーがメッセージを受信した日付及び時刻。

【００６５】

５．各行先リスティングに対するテーブル。

（ｉ）受信者ＭＴＡがメッセージを受信した時刻、及び／又はシステムが受信者ＭＴＡからＤＳＮレポートを受信した時刻。

（ｉｉ）その行先に対するメッセージの配達状態。配達受領書に引用される配達状態は、行先の配達状態のシステム内部記録をベースとしている。それらは、次のように書き表される。

・　状態がＦＡＩＬＥＤ（失敗）又はＵＮＤＥＬＩＶＥＲＡＢＬＥ（配達不能）である行先への配達は、「失敗」として受領書に記録される。

・　状態がＤＥＬＩＶＥＲＥＤ（配達済み）又はＤＥＬＩＶＥＲＥＤ－ＡＮＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）である行先への配達は、「メールサーバーへ配達済み」として受領書に記録される。

・　状態がＤＥＬＩＶＥＲＥＤ－ＴＯ－ＭＡＩＬＢＯＸ（メールボックスへ配達済み）である受信者への配達は、「メールボックスへ配達済み」として受領書に記録される。

これらのレポートの目的は、システムが達成できた配達の検証の形態を読者に正確に伝えることである。

【００６６】

６．ｅ－メールのオリジナル付属物と、それら付属物の個別メッセージダイジェストとのリスト。

７．オリジナルメッセージへの付属物のコピー。各オリジナル付属物は、受領書への付属物として添付される。

８．各行先へのメッセージの配達に含まれる全ＳＭＴＰダイアログの複写、要旨、又は複写の要約。

９．露呈される配達の細部又はメッセージの破棄を含む全受信ＤＳＮレポートの本体及び付属物の引用。

１０．ＤＳＮレポートの付属物としてシステムへ返送されたファイル。

【００６７】
受領書のこれら個別の全要素は、受領書内に含まれたそれら自身のメッセージダイジェスト又はデジタル符牒を有してもよい。更に、受領書は、計算されて受領書の一部分として添付される単一の全体的暗号化メッセージダイジェスト又はデジタル符牒を含んでもよく、従って、受領書内に含まれた全情報を認証するのに使用できる単一メッセージ認証コードを与える。受領書それ自体と、受領書内のＳＭＴＰダイアログ及びＤＳＮレポートは、タイムスタンプを含むので、受領書は、メッセージ受信者（１人又は複数）、メッセージ内容、並びに配達時刻（１つ又は複数）及びルート（１つ又は複数）の捏造不能な記録を含む。

【００６８】
ＭＵＡ通知の処理
ＭＵＡ通知は、ＭＴＡ　ＤＳＮと同様に、ＲＰｏｓｔ配達受領書内に収集して組み込むことができる。しかしながら、ＭＴＡ通知は、通常、配達の数時間以内に受信側ＭＴＡにより発生されるが、ＭＵＡ通知は、受信者が自分のＭＵＡのｅ－メールクライアントをオープンしそして受信したメールに対して何らかのアクションをとるまで発生されない。このため、本発明のこの実施形態では、ＭＵＡ通知は、ＭＴＡ通知とは別々に収集され、そしてＲＰｏｓｔ配達受領書とは個別の「ＲＰｏｓｔ読み取り受領書」において報告される。

【００６９】
上述したように構成されたメッセージヘッダにより引き出されるＭＵＡ通知は、共通のＲＰｏｓｔアドレス（例えば、「ｒｅａｄｒｅｃｅｉｐｔｓ@ＲＰｏｓｔ．ｃｏｍ」）へ返送され、そして各通知は、そのアドレスの名前フィールドに、このメッセージのオリジナル送信者のアドレスを含む。これは、以下に述べるように、ＲＰｏｓｔ読み取り受領書を発生するのに必要とされる唯一の情報であるから、システムは、これらのＭＵＡ通知が到着するときにそれを取り扱うことができ、オリジナルメッセージに関する情報をそのデータバンクに記憶する必要はない。

【００７０】
ＭＵＡ通知は、とりわけ、メッセージが受信者により読まれたこと、メッセージが受信者のターミナルに表示されたこと（読まれるかどうかに関わらず）、又はメッセージがオープンされずに削除されたことを報告する。ＭＵＡメッセージの内容又はフォーマットについてプロトコル支配される規格はない。システムは、ＭＴＡ　ＤＳＮに対するシステムの使用と同様に、ＭＵＡのテキストを検査し、それらの報告を解釈するように構成できる。しかしながら、本発明のこの実施形態では、ＭＵＡは、ＲＰｏｓｔサーバーにより評価又は解釈されず、むしろ、ＲＰｏｓｔにより認証できる形態で送信者へ送られて彼自身の評価を受ける。これを達成するために、システムは、「ＲＰｏｓｔ読み取り通知」としての形式のｅ－メールメッセージを作成し、これは、とりわけ、次のものを含む。

【００７１】
１．受信したＭＵＡ通知の主題ライン；
２．読み取り通知の本体として引用された受信ＭＵＡ通知の本体；
３．付属物として含まれた受信ＭＵＡ通知；
４．付属物（１つ又は複数）として含まれた受信ＭＵＡ通知に対する付属物（１つ又は複数）；
５．受信したＭＵＡ通知及びその通知に対する付属物（１つ又は複数）のメッセージダイジェスト；
６．日付及びタイムスタンプ；及び
７．文書及びその全ての内容に対して認証可能な日付スタンプされたデジタル符牒を与える少なくとも上記５及び６項の暗号化されたハッシュ。

【００７２】
受領書の破棄
本発明のこの実施形態の場合には、ＲＰｏｓｔ配達受領書及び読み取り通知の両方が、

登録メッセージのオリジナル送信者に送信される。これらの受領書は、暗号化されたハッシュでデジタル符牒が付けられるので、ＲＰｏｓｔは、以下に述べるように、この目的でＲＰｏｓｔにメッセージが提示されたときに、メッセージに含まれた情報を認証することができる。これは、受領書のコピーをその送信者へ送信すると（受領書を記録として保持するための送信者への命令と共に）、ＲＰｏｓｔは、メッセージ又はその配達に関するデータを保持する必要がもはやなく、このような全ての記録をシステムから抹消できることを意味する。従って、ＲＰｏｓｔは、オリジナルメッセージ又は受領書のコピーを保持する必要がない。公的記録メモリのこの経済性は、サービスプロバイダー側に大量のデータ記憶を必要とした公知の種々のメッセージ認証システムに勝る本発明の効果を与える。

【００７３】

この場合に、受領書のデータを保持する負担は、メッセージのオリジナル送信者に課せられる。それとは別に又はそれに加えて、第三者の検証ＲＰｏｓｔは、おそらく追加料金で、受領書の永久的コピー、或いは若干の又は全ての受領書データを記憶してもよい。受領書又はその一部分（１つ又は複数）は、磁気テープ、ＣＤ　ＲＯＭ、又は他の記憶装置形式を含む適当な公的記録用記憶装置に保持されてもよい。それとは別に又はそれに加えて、ＲＰｏｓｔは、受領書又はその一部分を、送信者又は送信者組織の制御のもとで、この目的に供された記憶システムに返送してもよい。

【００７４】

上述したように、ＲＰｏｓｔ受領書情報は、オリジナル送信者のメッセージ及びその付属物からの全てのデータを含む。システムのユーザが受領書をその記録に保持する負担を負いたくない（例えば偶発的なデータ損失のおそれから）が、それらのメッセージの内容を第三者ＲＰｏｓｔの手に入れさせたくもないという環境がある。従って、ＲＰｏｓｔは、送信者に保持されたメッセージのコピーが与えられたときにＲＰｏｓｔがメッセージの配達を認証及び検証するに必要とされる情報（例えば、送信者、構成の日付、メッセージダイジェスト、行先及び配達状態）のみをデータベースに記憶してメッセージの内容を破棄してもよい。

【００７５】

検証

メッセージの発信者が、ｅ－メールが送信され、配達され及び／又は読まれたという証拠を後日に要求する場合には、発信者がメッセージの受領書（１つ又は複数）をシステムのオペレータに提示する。

例えば、特定のメッセージが送信者１０から受信者１８へ送信されたことを証明するために、送信者１０は、受領書２０のコピーを、その受領書内に含まれた情報を検証する要求と共にＲＰｏｓｔへ送信する。これは、ＲＰｏｓｔにおける規定のメールボックス、例えば、ｖｅｒｉｆｙ@ＲＰｏｓｔ．ｃｏｍへ受領書を送信することによって行うことができる。次いで、ＲＰｏｓｔは、受領書が有効な受領であるかどうか決定する。受領書は、デジタル符牒が受領書の残り部分に一致し、そしてメッセージダイジェストがオリジナルメッセージの各対応部分に一致する場合に有効な受領書である。より詳細には、ＲＰｏｓｔは、メッセージ本体、付属物を含むメッセージの種々の部分、並びにＳＭＴＰ及びＤＳＮレポートを含む全メッセージに対してハッシュ関数を実行し、メッセージとされているもののコピーに対応する１つ以上のメッセージダイジェストを発生する。ＲＰｏｓｔは、メッセージとされているもののコピーにおけるメッセージダイジェスト（全メッセージダイジェストを含む）を、メッセージとされているもののコピーからＲＰｏｓｔが計算したメッセージダイジェストと比較する。全メッセージダイジェストは、受領書とされているものにおいてデジタル符牒として受け取られた全メッセージダイジェストを暗号解読するか、又はメッセージとされているもののコピーから計算された全メッセージダイジェストを暗号化することにより、比較することができる。デジタル符牒を含むメッセージダイジェストが一致する場合には、その受領書が、本物のＲＰｏｓｔ発生受領書である。良好なハッシュ関数が使用され、そして暗号化ハッシュ関数及びデジタル符牒暗号化アルゴリズムに使用されるキーが他の者に漏れていないと仮定すれば、受領書を提示する者により受

領書が「捏造」されていることは実質上不可能である。即ち、受領書は、ＲＰｏｓｔにより発生された受領書に違いなく、それ故、受領書に含まれたメッセージ、「へ／から」情報、配達の日付及び時刻、首尾良い配達の事実、メッセージが送られたルート、及び受領書内に含まれたＤＳＮ情報は、その情報の真のコピーに違いなく、正確なものである。次いで、ＲＰｏｓｔは、受領書内に含まれた情報の認証、検証及び確認を与えることができる。この確認は、ｅ－メール確認、ＲＰｏｓｔにより使用される方法に精通したＲＰｏｓｔ従業員からの供述証明書、宣誓証言及び裁判所における生の誓約証明書の形態、並びに他の証明書形態をとることができる。ＲＰｏｓｔは、種々の各確認業務に対して、送信者１０、受信者１８、又は他のエンティティに料金を課すことができる。又、ＲＰｏｓｔは、受領書とされているものの偽物に関して証明又は他の確認を与えることもできる。証明書は、連邦証拠規定(Federal Rules of Evidence)９０１（９）、９０１（１０）、８０３（６）、８０３（７）、１００１－１００４、１００６、７０２－７０６、それに対応する州の証拠規定、及び他の適用規定に基づいて与えることができる。

【００７６】

要約すれば、システムは、特定の内容を有する特定のメッセージが送信されたという利害関係のない第三者の証明に基づき、いつそれが送信され、誰がそれを送信し、誰がそれを受け取り、いつそれが読むためにオープンされ、そしていつそれが削除されたかについて確実な証拠を与える。この証拠は、例えば、契約書の作成、株の売買注文、及び他の多数の用途において、メッセージの内容及び配達について争議が生じたときにいつでも提出することができる。システムのオペレータは、受領書に含まれた情報の記録又はコピーを保存する必要なく、受領書自体に含まれた情報の正確さを立証することができる。

【００７７】

このシステムの重要な効果は、既存のＭＵＡを何ら変更せずにそれにより使用できることである。全ての計算、暗号化、ＥＳＭＴＰ質問及びダイアログ、ＤＳＮレポート収集、及び受領書の編集は、第三者のＲＰｏｓｔサーバーにより実行されるので、これら機能は、いずれも、ユーザの装置内で実行する必要がない。従って、ユーザは、システムの利点を迅速且つ容易に取り入れることができる。

上述した本発明の実施形態では、ＲＰｏｓｔサーバーが、それを通過する全メッセージの配達を登録する。それとは別に、ＲＰｏｓｔサーバーは、ある行先（例えば、組織の外部）を有するメッセージのみ、又はある送信者（例えば、顧客関係グループ）からのメッセージのみを登録してもよい。それとは別に又はそれに加えて、ＲＰｏｓｔサーバーは、メッセージの主題又は本体に区別キャラクタ又はストリングを有したメッセージのみを登録してもよい。例えば、サーバーは、送信者がメッセージの主題に「（Ｒ）」を含ませたメッセージのみを登録してもよい。他の全てのメッセージは、通常のインターネットＭＴＡのようにＲＰｏｓｔサーバー又は他の何らかのサーバーファンクションにより配達されてもよい。

【００７８】

この実施形態では、ＲＰｏｓｔは、種々の方法で収入を高めることができる。例えば、ＲＰｏｓｔは、メッセージ送信者１０又はその組織に、メッセージごとのベースで、キロバイトごとのベースで、毎月といった定期的定額ベースで、或いはそれらの組合せのベースで料金を課すことができる。又、ＲＰｏｓｔは、受領書の認証及び検証に料金を課すことができ、料金表は、求められる検証が単純な戻りｅ－メールであるか、書かれた供述書又は宣誓書であるか、宣誓証言又は法廷における誓約事実証明書であるか、或いは宣誓証言又は法廷における誓約専門証明書であるかに依存する。ユーザが、ＲＰｏｓｔに受領書のコピーを保持させるように選択した場合には、ＲＰｏｓｔは、項目当たり及び／又はキロバイト当たりの毎月記憶料金を課すことができる。

【００７９】

ＩＩ．出メッセージを登録するためのフローチャート

図２Ａないし２Ｇは、システムの第１実施形態の例示的オペレーションを示すフローチャートである。ソフトウェア及びｅ－メールプロトコルに精通した当業者であれば、他の

実施形態に適用するようにこのフローチャートを変更することができよう。
図２Ａ（前処理）は、登録サーバー（システム）により送信される前にメッセージと共に行われるステップを示す。
【００８０】
ｅ－メールメッセージを登録するために、ステップ２０１において、発信者／送信者／ユーザは、インターネットメールユーザエージェント（ＭＵＡ）を使用してｅ－メールメッセージを作成する。考えられるＭＵＡは、（１）クライアント側のｅ－メールプログラム、（２）サーバーベースのｅ－メールプログラム、（３）ウェブベースのｅ－メールサービス、及び（４）ウェブページを経て提出されるＨＴＭＬフォームを含む。メッセージは、参考としてここに取り上げるコメントの要求（ＲＦＣ）８２２、２０４６及び２０４７に説明された添付ファイルを含むことができる。ＲＦＣは、ネットワークプロトコル、手順、プログラム及びコンセプトに焦点を合わせて、コンピュータ通信の多数の観点について示すインターネットに関する一連の覚書である。
【００８１】
この実施形態において、システムは、送信者の出メールサーバーとして機能し、従って、送信者のメッセージは、送信者のＭＵＡによりＲＰｏｓｔサーバーへ直接転送される（ステップ２０２）。
ステップ２０３では、システムは、後で処理するために記憶されるオリジナルメッセージのコピーを形成する。
ステップ２０４では、システムは、メッセージがサーバーにより受け取られた時刻、メッセージのファイル付属物の名前とサイズ、メッセージの各行先の名前（もし分かれば）、各行先のインターネットアドレス、メッセージが行先のＭＴＡに配達された時刻（最初、この値はナルである）、及び各行先の配達状態を記録するユニットのような情報を含む記録をデータベースに形成する。
【００８２】
ステップ２０５において、各行先の配達状態が「ＵＮＳＥＮＴ（非送信）」にセットされる。
ステップ２０６において、システムは、メッセージ本体から作られるメッセージダイジェスト又はデジタル指紋(fingerprint)を発生して記憶する。
ステップ２０７において、システムは、メッセージに含まれる各付属物に対しハッシュ又はメッセージダイジェストを発生して記憶する。
ステップ２０８において、システムは、オリジナルメッセージの変更されたコピーを作成する。この第２のコピーにおいて（ステップ２０９）、メッセージのオリジナル主題ラインは、このコピーが登録されたことを示すように変更される（例えば、「登録済み」を前にぶら下げることにより）。
【００８３】
ステップ２１０において、システムによりメッセージが登録されたという通知が、システムのワールドワイドウェブサイトへのリンクと共にメッセージの本体に添付される。
ステップ２１１では、種々のＭＵＡにより確認された種々のヘッダフォーマットで読み取り通知を要求するｅ－メールヘッダが追加される。この通知の要求は、システムに関連したアドレス、例えば、「ｒｅａｄｒｅｃｅｉｐｔ@ＲＰｏｓｔ．ｃｏｍ」へ返送通知を指令する。又、これらのヘッダは、ＭＵＡ通知を送信しなければならないアドレスの名前フィールドにメッセージのオリジナル送信者のアドレスも含ませる。
前処理が完了すると、システムは、次いで、メッセージのコピーを、図２Ｂに示すように、各行先へ送信する。
【００８４】
図２Ｂは、登録されたメッセージを送信するのに必要なステップを示す。ステップ２２０に示したように、プロセスは、メッセージの各受信者に対して個別の送信を必要とする。
ステップ２２１では、システムは、名前がメッセージのオリジナル送信者であるが、ア

ドレスが、次のものから構成された「ＲＰｏｓｔ．ｃｏｍ」であるような送信者「から：」のものであるとしてメッセージを示すために、メッセージのワーキングコピーのヘッダフィールドを変更する。

ａ）返送ＭＴＡ通知（例えば、「ＲＣＰＴ」）を識別するのに使用されるストリング；

ｂ）送信されているメッセージを独特に識別するストリング；

ｃ）メッセージのこのコピーが送信される行先を独特に識別するタグ。

【００８５】

ステップ２２２では、現在送信されている行先のドメイン名を使用して、システムは、ドメイン名サーバーメール交換ルックアップを行って、このドメイン内のアドレスに対するメールを収集する役割を果たすＭＴＡ（１つ又は複数）のアドレスを見出す。

ステップ２２３では、システムは、行先のＭＴＡへの直接テルネット接続を行うように試みる。接続が失敗した場合には、システムは、再び接続を行うように試みる。システムが、この行先に対して最大数の再試みを越えないとすれば（２２７）、システムは、おそらく行先ドメインに対して別のＭＸサーバーを使用して接続を再び行うよう試みる（２２８）。

【００８６】

最大数の再試みの後、システムがこの行先のＭＴＡに接続できない場合には、システムは、ステップ２２６において、この行先の配達状態を「ＵＮＤＥＬＩＶＥＲＡＢＬＥ（配達不能）」として記録し、そしてこのメッセージをこの行先へ配達する試みを停止する。

行先のＭＴＡへ接続すると、システムは、その（Ｅ）ＳＭＴＰダイアログの記録をＭＴＡで行い始める（２２５）。

ステップ２２９では、システムは、「ＥＨＬＯ」グリーティングを発生することにより、行先ＭＴＡとの拡張ＳＭＴＰ（ＥＳＭＴＰ）交換を開始するように試みる。

【００８７】

行先ＭＴＳがＥＳＭＴＰをサポートする場合には、システムは、行先ＭＴＡがＳＭＴＰファンクションＶＥＲＩＦＹをサポートするかどうか決定する（２３０）。ＭＴＡがＶＥＲＩＦＹをサポートする場合には、システムは、行先アドレスがドメイン内の有効アドレスであるかどうか決定するよう試みる（２３１）。

アドレスが有効でない場合には、ステップ２３２において、システムは、この行先の配達状態を「ＦＡＩＬＵＲＥ（失敗）」と記録し、そしてこのメッセージをこの行先に配達するよう試みるのを停止する。

アドレスが有効であるか、又はＥＳＭＴＰサーバーがＶＥＲＩＦＹをサポートしない場合には、システムは、受信側ＭＴＡがＥＳＭＴＰサービスＤＳＮ（配達状態通知）をサポートするかどうか決定する（２３３）。

【００８８】

ＭＴＡがＥＳＭＴＰ　ＤＳＮをサポートする場合、システムは、配達が成功であるか失敗であるかをメッセージの名目上の送信者に通知するためのＥＳＭＴＰ要求と共にメッセージを送信する（２３４）。メッセージを送信すると、システムは、この行先の配達状態を「ＤＥＬＩＶＥＲＥＤ－ＡＮＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）」として記録する（２３５）。

受信側ＭＴＡが拡張ＳＭＴＰをサポートしない場合には、システムは、ＳＭＴＰを使用してメッセージを送信し（２３６）、そして行先の状態を「ＤＥＬＩＶＥＲＥＤ（配達済み）」として記録する（２３７）。

メッセージを配達すると、システムは、（Ｅ）ＳＭＴＰダイアログを記憶して、配達を、後で回復できるように記録し（２３８）、そしてメッセージを別の行先へ送信するよう試みる。

【００８９】

メッセージをその行先へ送信すると、システムは、メッセージの破棄に関する情報を収集するために多数の機能を実行しなければならない。図２Ｃは、受信者ＭＴＡにより返送されるＭＴＡ通知をシステムが処理するところのプロセスを示す。

図２Ｂのステップ２２１に示された送信されたメッセージのヘッダに使用されるフォーマットにより、ＭＴＡメッセージ通知は、サーバーにおける架空のローカルアドレスに配達される。システムは、これらの通知を、そのアドレスに埋め込まれたストリング（例えば、「ｒｃｐｔ」）により検出することができる（２４１）。ステップ２４２に示すように、アドレスをパージングすることにより、システムは、どの行先へのどのメッセージが受信通知を促したか決定することができる。

【００９０】

ステップ２４３では、システムは、ＭＴＡが配達の成功を報告するか、配達の失敗を報告するか、又はメッセージが別のサーバーへ中継されたことを報告するかを指示するフレーズに対して、受信したＭＴＡの主題ライン及び本体を走査する。

ステップ２４３におけるプロセスが、通知が配達の成功を報告することを表わしている場合には、システムは、ステップ２４５に示すように、当該メッセージの当該行先の配達状態を「ＤＥＬＩＶＥＲＥＤ－ＴＯ－ＭＡＩＬＢＯＸ（メールボックスへ配達済み）」に変更する。

ＭＴＡ通知が配達失敗を報告することをシステムが決定した場合には、システムは、当該メッセージの当該行先の配達状態を「ＦＡＩＬＵＲＥ（失敗）」に変更する（２４７）。

【００９１】

メッセージが別のサーバーへ中継されたことをＭＴＡ通知が指示することをシステムが決定した場合には、システムは、ステップ２４９に示すように、当該メッセージの当該行先の配達状態を「ＲＥＬＡＹＥＤ（中継済み）」に変更する。

ＭＴＡ通知を処理すると、システムは、このメッセージ及び全ての付属物をセーブし、それらを後で呼び戻して、この行先の受領書の作成に使用できるようにする（２５０）。

時々、図２Ｄに示すように、システムは、各メッセージの状態を検査して、メッセージの行先ごとにおそらく受信するであろう全ＭＴＡ通知をシステムが回復したかどうか決定し、次いで、メッセージの受領書を作成するように進む。

【００９２】

システムは、メッセージの各行先の配達状態を検査する。

行先が配達状態「ＵＮＳＥＮＴ（非送信）」を有する場合には、メッセージの処理が完了していない（２５２）。

行先の配達状態が「ＤＥＬＩＶＥＲＥＤ－ＡＮＤ－ＷＡＩＴＩＮＧ－ＦＯＲ－ＤＳＮ（配達済みでＤＳＮを待機している）」である場合には、システムは、ステップ２５４に示したように、メッセージを配達して以来の時間がシステムの待機周期（例えば、２４時間）を越えない限り、この行先に対する処理を完了とはみなさない。

【００９３】

行先の配達状態が「ＤＥＬＩＶＥＲＥＤ（配達済み）」である場合には（２５７）、システムは、システムのオペレータが行先ＭＴＡから受け取った配達失敗通知を充分に処理する時間周期（例えば、２時間）が経過したならば（２５８）、この行先の処理を完了とみなす。

他の行先配達状態（例えば、「ＦＡＩＬＥＤ（失敗）」、「ＵＮＤＥＬＩＶＥＲＡＢＬＥ（配達不能）」、「ＤＥＬＩＶＥＲＥＤ－ＴＯ－ＭＡＩＬＢＯＸ（メールボックスへ配達済み）」）は、完了した処理を有するものとして処理される。

いずれかのメッセージ行先の処理が完了でない場合、システムは、何のアクションもとらず、システム内の他のメッセージを考慮することに移行する（ステップ２５５）。

【００９４】

しかしながら、ステップ２５９に示すように、メッセージの各行先の処理が完了である場合には、システムは、メッセージに対する配達受領書を発生する。

図２Ｅに例示されたように、受領書は、次のものを含む。

ブロック２７１における管理目的の識別子。この識別子は、送信者ＩＤに対するリファレンス、及び／又はシステムにより受信された送信者メッセージのインターネットメ

ッセージＩＤの値であるか又はそれを含む。
　　ブロック２７２のように、オリジナルメッセージ１２の引用された本体、及びその意図された受信者のｅ－メールアドレスも含まれる。
　　ブロック２７３のように、各受信者リストのテーブルは次のものを含む。
・　受信者のＭＴＡがメッセージを受信する時刻、及び／又はシステムが受信者のＭＴＡからＤＳＮを受信する時刻。
・　その行先に対するメッセージの配達状態レポート、即ち「メールサーバーへ配達済み」、「メールボックスへ配達済み」、「中継済み」、「配達失敗」、「配達不能」。
【００９５】
　　ブロック２７４のように、ｅ－メールのオリジナル付属物、及びそれらの個別のハッシュ値又はメッセージダイジェストのリスト。
　　ブロック２７５のように、各行先へのメッセージの配達に含まれた全ＳＭＴＰダイアログの複写、又は複写の要約。
　　ブロック２７６のように、明らかとなるメッセージの配達又は破棄の詳細を含む全受信ＤＳＮの本体及び付属物からの引用。
　　ブロック２７７のように、システムは、オリジナルメッセージの全付属物のコピーを受領書に添付し、そしてブロック２７８のように、システムは、システムへ返送されるファイルを、ＤＳＮへの付属物として付加的に添付する。
【００９６】
　ステップ２７９において、受領書のテキストを発生すると、システムは、ｅ－メールメッセージに対する第１ハッシュ、及び受領書の本体への付属物に対する第２ハッシュ（１つ又は複数）を発生し、そしてシステムのオペレータしか知らない暗号キーを使用して各ハッシュに対するデジタル符牒を計算する。暗号は、例えば、参考としてここに取り上げるザ・データ・エンクリプション・スタンダード、ナショナル・インスティテュート・オブ・スタンダーズ・アンド・テクノロジー出版のフェデラル・インフォメーション・プロセッシング・スタンダード・パブリケーション４－２（ＦＩＰＳ　ＰＵＢ４６－２）に掲載されたデータ暗号化規格を使用することができる。或いは又、ハッシュ地を暗号化する他の既知の又は新規な方法を使用することもできる。
　ステップ２８０では、暗号化されたハッシュが「文書デジタル符牒」としてメッセージの終わりに添付される。
【００９７】
　ステップ２８１では、ここで完了している受領書２０が、送信者の記録に対して保持されるアドバイスと共に、ｅ－メールにより送信者へ送信される。ステップ２８２では、システムが、ここで、オリジナルメッセージ、付属物及びＤＳＮの全コピーを削除できる。或いは又、受領書を送信者に送信するのではなく、システムが受領書を記憶してもよいし、又は送信者及びシステムの両方が受領書を記憶することもできる。
　ＭＵＡ通知は、受信者の意志だけで、そして受信者が受信メッセージに対してあるアクションをとるときだけ返送されるので、システムの実施形態は、これら返送メッセージを、ＭＴＡ通知とは異なるやり方で処理するよう選択できる。
【００９８】
　図２Ｆは、これらのＭＵＡ通知をシステムによりいかに処理できるかを示す。ＭＵＡ通知は、図２Ａのステップ２１１のように、出て行くメッセージに種々のヘッダを含ませることにより、システムにより懇請される。これらのヘッダは、この目的に対して別に設定されたシステムアドレス（例えば、「ｒｅａｄｒｅｃｉｅｐｔ@ＲＰｏｓｔ．ｃｏｍ」）へ通知を送信するように適合ＭＵＡに指令する。又、これらヘッダは、この返送アドレスの「名前」フィールドに、メッセージのオリジナル送信者のｅ－メールアドレスも使用する。従って、ステップ２８６では、ＭＵＡ通知がｒｅａｄｒｅｃｅｉｐｔ@ＲＰｏｓｔ．ｃｏｍに返送されるときに、システムは、通知のアドレスを検査することにより、読み取り通知を送信しなければならないアドレスを決定することができる。
【００９９】

行先ＭＵＡから読み取り受領書が到着すると、システムは、ステップ２８７において、受信したＭＵＡ通知の主題をその主題として含みそして受信したＭＵＡ通知の本体をそのメッセージ本体に組み込む読み取り受領書を発生する。

ステップ２８８では、システムは、ＭＵＡ受領書を付随するファイルを受領書に添付する（通常、これらは、オリジナルｅ－メールの配達又は破棄の詳細及びそれに対する識別参照を含む）。

【０１００】

ステップ２９８では、システムは、受領書に添付されるファイルに対してハッシュを発生し、そしてこのハッシュを受領書の本体に記録する。

ステップ２９０では、システムは、受領書の本体及びその付属物に対するハッシュを発生し、このハッシュを暗号化し、そしてその結果を「文書デジタル符牒」としてメッセージに添付する。

ステップ２９１では、システムは、それにより得られる受領書をメッセージの送信者へ送信する。ステップ２９２では、この受領書を送信すると、システムは、トランザクションの全内部記録を削除する。

【０１０１】

ＩＩＩ．第２メールサーバーとしてのＲＰｏｓｔの実施形態

図３は、ＲＰｏｓｔサーバーがユーザの一次ＭＴＡとして働かず、別のＭＴＡと共同する本発明の第２実施形態のシステム図である。この実施形態では、送信者は、出メッセージ、メッセージ主題又はメッセージアドレスにある形式のフラグを含ませることにより特定の出メッセージを登録するよう選択できる。例えば、送信者がメッセージの主題に記号「（Ｒ）」を含ませた場合及びその場合だけ、送信者のＭＴＡは、メッセージを、ＲＰｏｓｔサーバーを経て送信するように向けて、受領書を発生させる。

この実施形態では、ＲＰｏｓｔのオペレータは、送信者ＭＴＡごとのメッセージ及び／又はキロバイトごとの送信のオペレータから収入を受け取る。

【０１０２】

ＩＶ．ＲＰｏｓｔへのＣＣの実施形態

図４は、カーボンコピー（ｃｃ）がＲＰｏｓｔサーバーへ送信される第３実施形態のシステム図である。この実施形態では、ユーザ又はメッセージ送信者１０は、標準的なＭＵＡ及び標準的なＭＴＡを変更なしに使用することができる。メッセージ送信者１０は、メッセージ本体及びある数の付属物を有するｅ－メールを構成し、そしてそれを、カーボンコピー（ｃｃ）及び必要に応じてブラインドカーボンコピー（ｂｃｃ）と共に、メッセージ受信者１８へアドレスする。更に、メッセージ送信者１０は、ｃｃをＲＰｏｓｔにアドレスする。ＲＰｏｓｔサーバー１４は、上述したようにメッセージにタグ付けを行い、そして付属物を含むタグ付けされたメッセージを受信者のＭＴＡ１６及び指定のｃｃへ送信する。このようなコピーを受け取ると、ＲＰｏｓｔサーバー１４は、そのコピーのｅ－メール確認受領書を送信する。

【０１０３】

受信者１８及び他のメッセージ行先は、ここで、同じメッセージの２つのバージョンを受け取る。即ち、送信者１０から直接受け取られるメッセージの第１バージョンと、ＲＰｏｓｔから転送された第２のタグ付きバージョンである。メッセージのタグ付きバージョンが受信者ＭＴＡ１６により首尾良く受け取られたという確認をＲＰｏｓｔが受信者ＭＴＡ１６から受信すると、ＲＰｏｓｔサーバー１４は、上述したように、メッセージ受領書２０を構成し、そしてその受領書を送信者１０へ記録のために送信する。

メッセージ発信ドメイン又は個々のメッセージ送信者に対して口座を確立し、そしてメッセージごと、キロバイトごと、月ごと、又はそれらの組合せでユーザの口座に課金することにより、収入を発生することができる。又、受領書に広告を入れたり、上述したように認証及び検証サービスを行ったりすることから収入を発生することもできる。

【０１０４】

Ｖ．ウェブサイトの実施形態

図５は、第４の実施形態のシステム図である。この実施形態において、ＲＰｏｓｔサーバー１４には、ユーザがメッセージを構成するところのウェブサイトが関連される。メッセージ送信者１０は、ＲＰｏｓｔウェブサイトに訪問し、そして希望の「ｔｏ（宛先）」、「ｃｃ」、「ｂｃｃ」、「主題」、及びメッセージテキスト情報を入力することによりウェブサイトにおいて自分のメッセージを構成する。付属物は、標準的なブラウザ及びウェブサーバに使用できる特徴を使用することにより追加できる。この実施形態では、送信者は、登録受領書を送信するアドレスを付加的に与えねばならない。ＲＰｏｓｔサーバー１４は、送信者ＭＴＡを経て送信者１０へ受領書を送信する。

メッセージ発信ドメイン又は個々のメッセージ送信者に対して口座を確立し、そしてメッセージごと、キロバイトごと、月ごと、又はそれらの組合せでユーザの口座に課金することにより、収入を発生することができる。又、受領書に広告を入れたり、上述したように認証及び検証サービスを行ったりすることから収入を発生することもできる。

【０１０５】

ＶＩ．ウェブベースＭＵＡの実施形態

図６は、第５実施形態のシステム図である。この実施形態では、ＲＰｏｓｔサーバー１４に、ウェブベースのメールユーザエージェントが関連される。ユーザがウェブブラウザを経てメールを構成できるようにするのに加えて、このようなＭＵＡは、ウェブサーバーサイトに記憶されたメッセージを表示するブラウザ・ビューアブル・メールボックスを加入者に与える。このようなサービスを受ける加入者は、ユーザ名及びパスワードでメール口座にアクセスすることができる。この実施形態では、メッセージ送信者１０は、ＲＰｏｓｔウェブサイトに訪問し、ユーザ名及びパスワードを入力することによりウェブベースｅ－メール口座にアクセスし、そしてこのメッセージを構成し、これは、ＲＰｏｓｔサーバー１４へ配達するために搬送される。ＲＰｏｓｔサーバーにより発生された受領書は、加入者の口座に関連したウェブベースのメールボックスへ返送される。

他の実施形態において使用できる収入源に加えて、この実施形態では、オペレータは、ウェブベースのメールボックスに保持された受領書に対し記憶料金を課すことができる。

【０１０６】

これらの全実施形態において、受領書は、次のことに対する証拠として働く。

（１）発信者がｅ－メールメッセージを送信した。

（２）メッセージがある時刻に送信された。

（３）ｅ－メールがある受信者（１人又は複数）へアドレスされた。

（４）ｅ－メールが、その意図された受信者（１人又は複数）各々のｅ－メールボックスに配達された。

（５）ｅ－メールがある時刻に配達された。

（６）ｅ－メールがあるネットワークルートで配達された。

（７）ｅ－メールメッセージ及びその付属物が、受領書に記録された特定の内容を有していた。

【０１０７】

更に、ある環境のもとにあるシステムは、次のことに対する証拠として使用できる個別の受領書を発生する。

（１）ｅ－メールが、受信者のメールユーザエージェント（ＭＵＡ）を介して検査された。

（２）受信者が、メッセージに応答して、あるアクションを行い、例えば、特定の時刻にｅ－メールを読むか又は削除した。

他の実施形態と同様に、この実施形態は、電子メッセージの配達及び完全性についてシステムの利害関係のない第三者のオペレータにより立証及び検証できる文書化された証拠を形成する。換言すれば、システムは、ｅ－メールを、特定のｅ－メールメッセージが送信されたこと、それが首尾良く配達されたこと、そしていつ、いかに配達されたかを証明するために後で使用できる登録（書留）ｅ－メールに変換するものとして考えることができる。

【０１０８】
争議がいつも生じるとすれば、その争議は、システムにより発生される受領書により解決することができる。というのは、システムのオペレータが、システムから発生されたものとして受領書が本物であることを決定できるように、受領書がエンコードされるからである。その後、システムのオペレータは、受領書自体に含まれた情報のみに基づいて、本物の受領書に含まれる情報の正確さを立証することができ、オペレータが、受領書に含まれた情報の記録又はコピーを保存する必要はない。
これらの利益に加えて、システムにより発生される受領書は、システムを経て送信されるであろう資料の存在及び著者であることの証拠としても有用である。更に、システムは、インターネットのｅ－メールクライアントプログラム／ＭＵＡから使用でき、従って、付加的なソフトウェアは必要でないので、使用が容易である。
【０１０９】
受領書を有効性確認するためのフローチャート
図７は、受領書を有効性確認するための例示的方法を示すフローチャートである。メッセージの送信者が、ｅ－メールが送信されて配達された（及び／又は読まれた）という証拠を要求する場合には、ステップ７００において、送信者が、メッセージに対応する受領書（１つ又は複数）をシステムのオペレータに提示する。次いで、システムのオペレータは、ステップ７０２において、受領書に添付された文書デジタル符牒を分離して暗号解読する。ステップ７０３では、オペレータは、付属物を含む文書の残り部分のハッシュを発生する。
ステップ７０４において、現在のハッシュ値が、暗号解読されたハッシュ値に一致しない場合には、システムは、ＲＰｏｓｔが、その受領書を、その受領書に記載されたメッセージの配達又は内容の正確な記録として認証できないことを示すレポートを発生する。
【０１１０】
暗号解読されたハッシュがメッセージの現在ハッシュに等しい場合には、システムは、ステップ７０６において、メッセージの本体に含まれた情報が、受領書がシステムに通されて以来、不変であることを保証できる。オリジナルメッセージが付属物を含まない場合には、システムは、受領書がメッセージ内容の正確な記録でありそしてＲＰｏｓｔサーバーにより配達されたものであることを保証するレポートをここで発生することができる。
受領書が、オリジナルメッセージが付属物を含んでいたことを報告する場合には、受領書が、各付属物の名前及びハッシュ値も記録する。受領書を発生する場合に、オリジナルメッセージの全ての付属物は、受領書に不変に添付される。従って、システムは、このような各添付ファイルに対し、添付ファイルのハッシュを発生し（７０８）、そしてそれを、受領書の本体に記録されたハッシュ値と比較する（７０９）。
【０１１１】
ファイルの計算されたハッシュ値が、受領書に含まれた値に一致する場合には、システムは、受領書に添付されたファイルが、最初に配達されたメッセージに添付されたものと同じであることを保証できる。ハッシュが一致しない場合には、システムは、受領書に添付されたファイルが、オリジナルメッセージに添付されたファイルと同じであることを保証できないと報告する。
オリジナルメッセージに添付された各ファイルに対しこの計算を実行すると、システムは、受領書及び各添付ファイルが本物である（７１０）ことを報告するか又は有効性に欠陥がある（７１２）ことを報告するレポートを作成する。
その評価を完了すると、システムは、受領書及びその全ての付属物のコピーを、それが発生したレポートに添付し、そしてそれを、ｅ－メールにより、有効性確認のためにレポートを提出したユーザの戻りアドレスに送信する。
【０１１２】
ＶＩＩ．インバウンドｅ－メールの登録
図８は、到来するｅ－メールが登録される本発明の別の実施形態を示すシステム図である。この実施形態において、メッセージ送信者６０は、ｅ－メールメッセージ７０を送信

する。送信者のＭＴＡ６２は、メッセージ７０をインターネットに通常の通りに送信する。しかしながら、この実施形態では、ＲＰｏｓｔは、到来するｅ－メールを登録するようにサービス加入者／受信者６８と契約する。その協約に基づき、ＲＰｏｓｔは、ネットワーク・ソルーションズ・インク（ＮＳＩ）又は他のドメイン名当局により、受信者６８に対するメール受信者（ＭＸサーバー）として指定される。これは、送信者のＭＴＡ６２により実行されるドメイン名サービス（ＤＮＳ）が、ＲＰｏｓｔのＩＰアドレスを受信者のＩＰアドレスとして返送するようにさせ、次いで、送信者のＭＴＡ６２がｅ－メールメッセージをＲＰｏｓｔサーバー６４へ送信するようにさせる。ＲＰｏｓｔサーバー６４は、受信者６８に対するＳＭＴＰ、ＰＯＰ、ＰＯＰ３又はＩＭＡＰ　ＭＴＡ（集合的に「ＰＯＰメールサーバー」）として働く。ＳＭＴＰ、ＰＯＰ及びＩＭＡＰ　ＭＴＡは、参考としてここに取り上げるＲＦＣ８２１、ＳＭＴＰプロトコル、ＲＦＣ１９３９ポストオフィスプロトコル、第３版（旧ＲＦＣ１７２５）、及びＲＦＣ２０６０　ＩＭＡＰ（インターネットメッセージアクセスプロトコル）、第４版、改訂１（旧ＲＦＣ１７３０）により支配される。

【０１１３】

ＲＰｏｓｔサーバー６４は、オリジナルメッセージ７０の登録バージョン７４を準備し、そしてその登録バージョン７４を、オリジナルメッセージ７０に代わって又はそれに加えて、受信者６８のインボックスに入れる。この登録バージョンは、ｅ－メール受領書に関連して上述した全ての検証及び情報特徴並びにオプションを有する。この情報は、メッセージ本体及びテキストの各々に対する個々のメッセージダイジェスト、「へ／から」情報、他のヘッダ情報、各付属物、全メッセージダイジェスト、デジタル符牒、メッセージルーティング情報、及びタグを含むことができるが、これらに限定されない。図６に示したメッセージ７０の登録バージョン７４は、ヘッダ情報を含むメッセージ本体、付属物、その各々の個別メッセージダイジェスト、及びデジタル符牒又は暗号化されたメッセージダイジェストを含む。ハッシュ関数及び暗号化は、システムのオペレータしか知らないプライベートなフレーズ又はプライベートキーを使用して実行される。登録バージョン７４は、点検のために又は受信者のＭＵＡを経てダウンロードするために受信者６８に使用できるようにされる。

【０１１４】

ＲＰｏｓｔサーバーは、確認ｅ－メール７２をメッセージ送信者６０へ任意に送信することができる。確認メッセージ７２は、メッセージが受け取られそして登録されたことを指示する簡単なテキストメッセージでよい。又、確認メッセージ７２は、「あなたのｅ－メールメッセージは、２０００年３月２４日の午後２：０５に受信されました。メッセージのデジタル符牒は、［１２８ビットデジタル符牒］です。更に詳細な情報については、当方のウェブサイトｗｗｗ．ＲＰｏｓｔ．ｃｏｍにおいで下さい。」というメッセージも含むことができる。それとは別に又はそれに加えて、確認メッセージ７２は、登録バージョン７４に含まれた全ての情報を含むこともできる。

【０１１５】

従って、システムは、メッセージ受信者６８に、受領書７４又は他の検証可能な確認を与える。即ち、

（１）受信者がｅ－メールメッセージを受信した。

（２）メッセージがある時刻に受信された。

（３）ｅ－メールがある送信者からアドレスされた。

（４）メッセージは、あるネットワークルートを経て配達されるとされる。

（５）ｅ－メールメッセージ及びその付属物は、特定の内容を有していた。

従って、システムは、ある内容を有しそしてある送信者から来たことをそれ自体表わしている特定の電子メッセージ及び文書が受信者に配達されたというシステムのオペレータにより立証できる証拠を与える。

【０１１６】

図９は、インバウンドメールを登録する一例を示すフローチャートである。ステップ９

０１において、ＲＰｏｓｔサーバー６４は、新たなｅ－メールメッセージを受信する。ステップ９０２では、システムは、メッセージのヘッダ及び付属物を含むメッセージの内容のハッシュ／デジタル符牒を発生する。更に、システムは、各メッセージ付属物に対して個別のハッシュを発生することができる。ステップ９０３では、システムは、システムのオペレータしか知らない暗号キーを使用してハッシュ（１つ又は複数）を暗号化する。ステップ９０４では、それにより得られる暗号化されたハッシュ（１つ又は複数）がメッセージの本体に添付される。次いで、ステップ９０５において、変更されたメッセージは、点検のため、又は受信者ＭＵＡを経てダウンロードするために使用できる。

【０１１７】

図１０は、受信された登録ｅ－メールメッセージを有効性確認する一例のフローチャートである。ステップ１０００において、特定の内容をもつｅ－メールが特定の時刻に受信された証拠をメッセージの受信者が要求する場合に、受信者は、ｅ－メールメッセージ７０の登録バージョン７４（図８）のコピーを検証のためにシステムのオペレータに提示することができる。メッセージを検証するために、ステップ１００１において、システムは、メッセージに添付された文書デジタル符牒を分離して暗号解読する。ステップ１００２では、システムは、文書の残り部分のハッシュを発生し、そしてメッセージに添付された各ファイルに対してハッシュを発生する。ステップ１００３及び１００４において、それらのハッシュが比較される。文書のハッシュが、暗号解読されたハッシュに一致する場合には、メッセージ及びその付属物は、システムに通さねばならず、そして受信者に配達されて以来、変更されていてはならない。

【０１１８】

ｅ－メールが変更されていないことが決定されると、システムのオペレータは、次のことを保証できる。

（１）ｅ－メールが、ある時刻にシステムにより受信された。

（２）ｅ－メールが、あるインターネットルートを経てシステムに到着するとされた。

（３）ｅ－メールが、ある送信者からのものとされた。

（４）ｅ－メール及びその付属物が、それらが現在含む特定の内容で配達された。

一方、ステップ１００６では、ハッシュ値が一致しない場合、オペレータは、ｅ－メールが本物であること、即ちｅ－メールが、システムによって受信されたｅ－メールの正確なバージョンであることを保証できない。

【０１１９】

図１１は、電子ツールを利用するビジネス（ｅ－ビジネス）によって本発明がいかに使用されるかを示す。ｅ－ビジネス３０は、顧客３４へ到来する及び顧客３４から出て行く全てのｅ－メールメッセージを登録するようにシステムを使用することができる。この場合に、システムは、ポストオフィスプロトコル（ＰＯＰ）サーバー３６及び簡単なメール転送プロトコル（ＳＭＴＰ）サーバー３８を備えている。例えば、ｅ－ビジネス３０は、そのウェブサイトを顧客へのｅ－メール形態に設定し、そして顧客３４から問合せ及び苦情４０を転送することができる。登録された問合せ、苦情、注文、購入のオファー及び他の情報４６は、システムによりｅ－ビジネス３０へ送信される。次いで、受領書がＳＭＰＴサーバー３８を経て顧客３４へ送られる。このように、顧客が通信を送ったかどうかそしてそれが何を含んでいたかに関して何の問題もない。更に、ｅ－ビジネスは、ＲＰｏｓｔサーバーを通してウェブサイト３２を設定し、顧客との各通信を登録することができる。換言すれば、ウェブサイトを経て、フォームデータ注文４２及び自動応答４４を、システムサーバーを介して登録することができ、更に、ｅ－ビジネスにより顧客３４に送られる確認、収集通知、顧客サポート及び特殊なオファー４８を登録できると共に、何が、いつ、誰によって注文されたかについての論争を排除するために顧客に送られた確認を登録することができる。必要であれば、同じ受領書を、顧客３４及びｅ－ビジネス３０の両方に与えることができる。或いは又、ＰＯＰサーバー３６及びＳＭＴＰサーバー３８の機能を単一のシステムサーバーにおいて結合することができる。

【０１２０】

ＰＯＰは、ｅ－メールサーバーからｅ－メールを検索するのに使用されるプロトコルである。多くのｅ－メールアプリケーション（時には、ｅ－メールクライアントとも称される）がＰＯＰプロトコルを使用するが、そのあるものは、新規なインターネットメッセージアクセスプロトコル（ＩＭＡＰ）を使用することができる。ＰＯＰ２と称されるＰＯＰの１つのバージョンは、メッセージを送信するためのＳＭＴＰを必要とする。新規なバージョンであるＰＯＰ３は、ＳＭＴＰと共に、又はＳＭＴＰなしで使用することができる。ＳＭＴＰは、サーバー間でｅ－メールメッセージを送信するためのプロトコルである。インターネットを経てｅ－メールを送信する多数のｅ－メールシステムは、ＳＭＴＰを使用して、あるサーバーから別のサーバーへメッセージを送信し、メッセージは、ＰＯＰ又はＩＭＡＰのいずれかを使用してｅ－メールクライアントにより検索することができる。更に、ＳＭＴＰは、一般に、メールクライアントからメールサーバーにメッセージを送信するのに使用される。ｅ－メールサーバーは、種々のプロトコルを使用して、インターネットと通信することができる。通常に使用されるプロトコルは、ＳＭＴＰ、ＰＯＰ３及びＩＭＡＰ４を含む。サーバーの反対端にメール読者がいる。メールサーバーは、ＳＭＴＰを経てメッセージを受信するので、ｅ－メール読者は、ＳＭＴＰを使用してメールサーバーにｅ－メールを送信する。同様に、メールサーバーは、ＰＯＰ３及び任意にＩＭＡＰ４を使用してメッセージを送信するので、メール読者は、ＰＯＰ３又はＩＭＡＰ４プロトコルを使用することによりメールサーバーからメッセージを受信する。

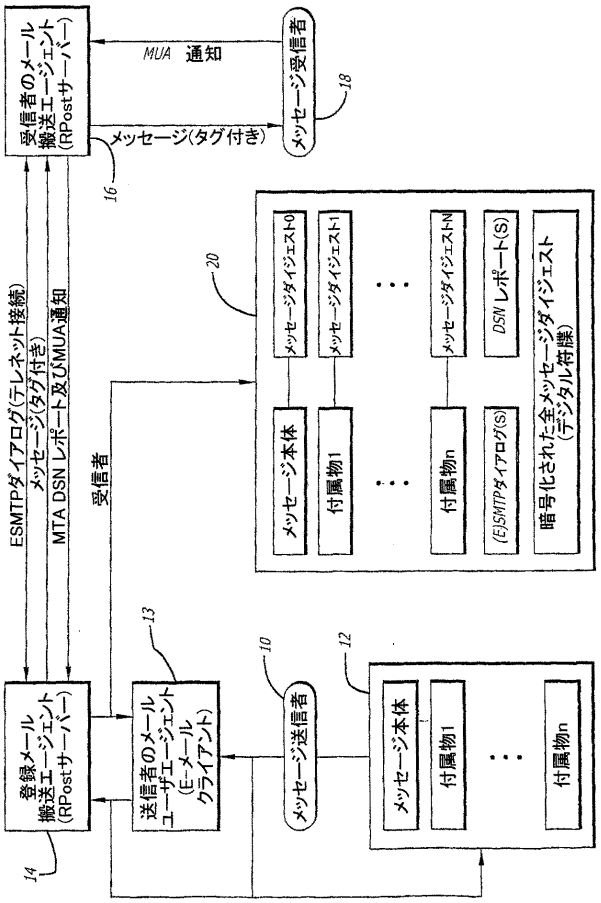
【０１２１】

以上、ｅ－メールが送信及び／又は受信されたことを検証するためのシステム及び方法について一般的に説明したが、本発明は、電子メッセージネットワーク又は電子ゲートを経て送信できるいかなる電子メッセージにも適用することができる。電子メッセージは、テキスト、オーディオ、ビデオ、グラフィック、データ、及び種々のファイル形式の付属物を含む。ここに教示した方法及び技術は、サーバー及び他のコンピュータにプログラムすることができ、そして本発明を実施するコンピュータプログラムは、ＣＤ　ＲＯＭ、ＲＡＭ、ハードドライブ及び磁気テープを含む（これに限定されない）コンピュータ読み取り可能な媒体に書き込むことができる。本発明によるｅ－メール登録サービスは、インターネットサービスプロバイダー（ＩＳＰ）サービスと共に束ねられて、単一プロバイダーＩＳＰ解決策を会社及び他の企業クライアントに提供することができる。上述した発明の実施は、ソフトウェ分野の当業者の熟練度の範囲内である。

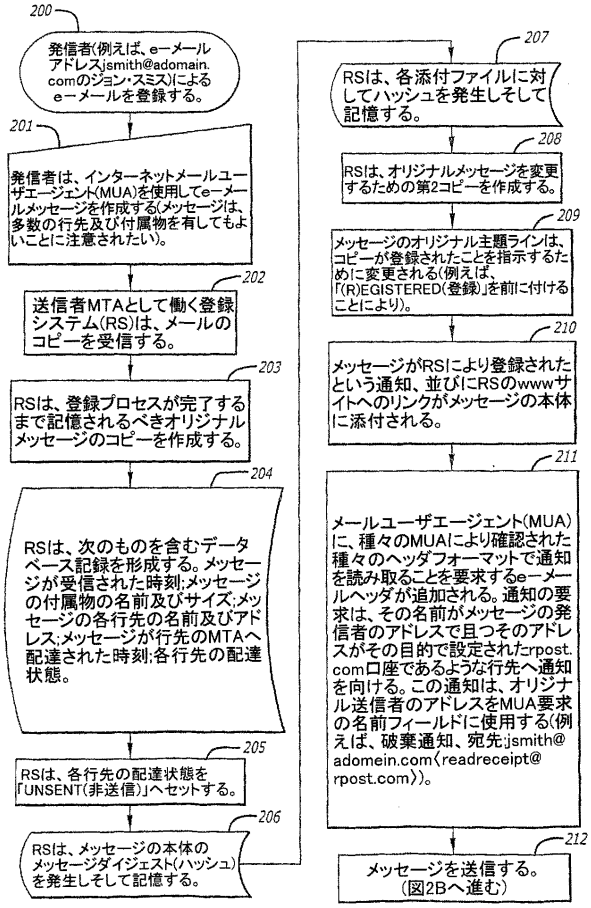
【０１２２】

従って、本発明は、その好ましい実施形態及び図面に関連して詳細に説明したが、本発明の精神及び範囲から逸脱せずに本発明の種々の応用及び変更がなされ得ることが当業者に明らかであろう。従って、上述した詳細な説明及び添付図面は、本発明を何ら限定するものではなく、本発明は、特許請求の範囲及びその等効物のみによって限定される。請求の範囲において、「手段」という語を含む請求項は、３５ＵＳＣ、第１１２条、第６項に基づいて解釈されるべきであり、そして「手段」という語を含まない請求項は、３５ＵＳＣ、第１１２条、第６項に基づいて解釈されるべきでない。

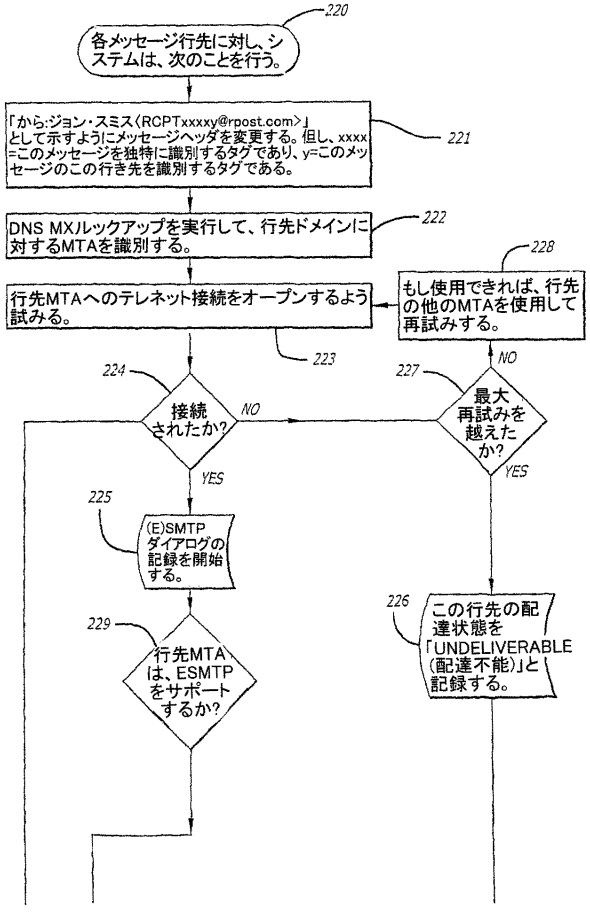
【図１】



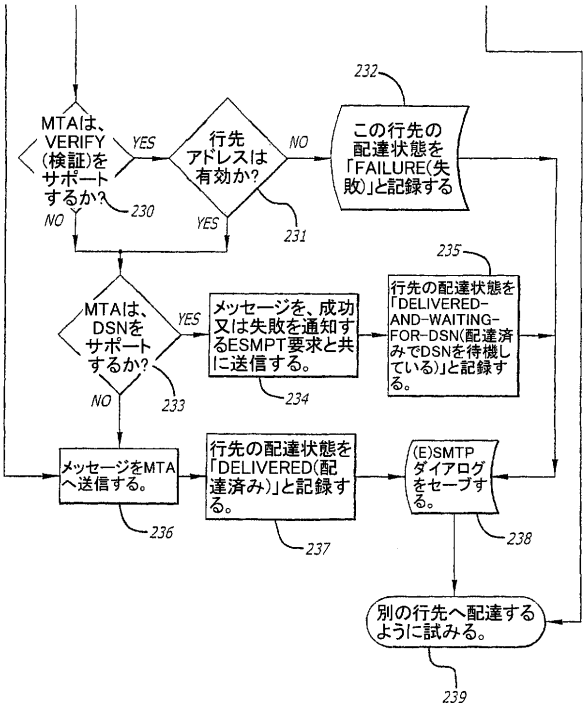
【図２Ａ】



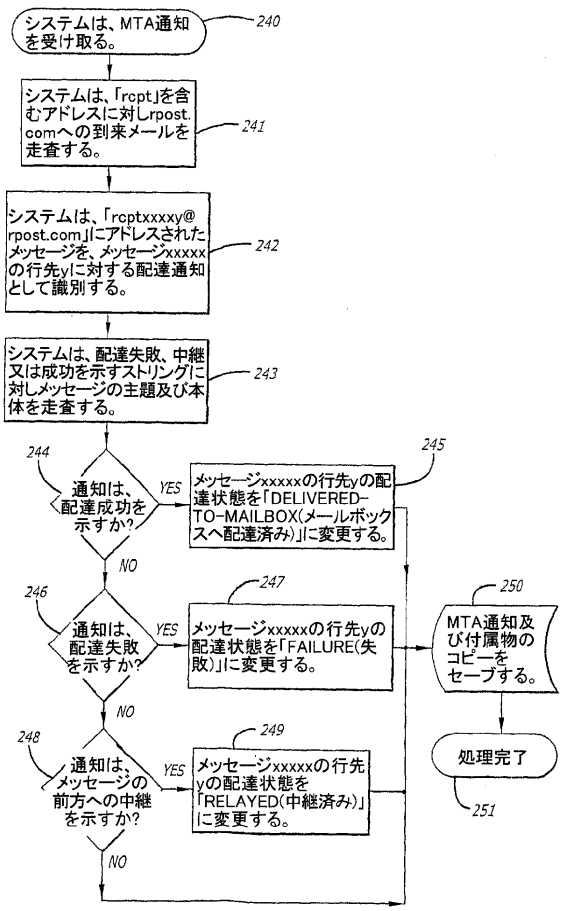
【図２Ｂ－１】



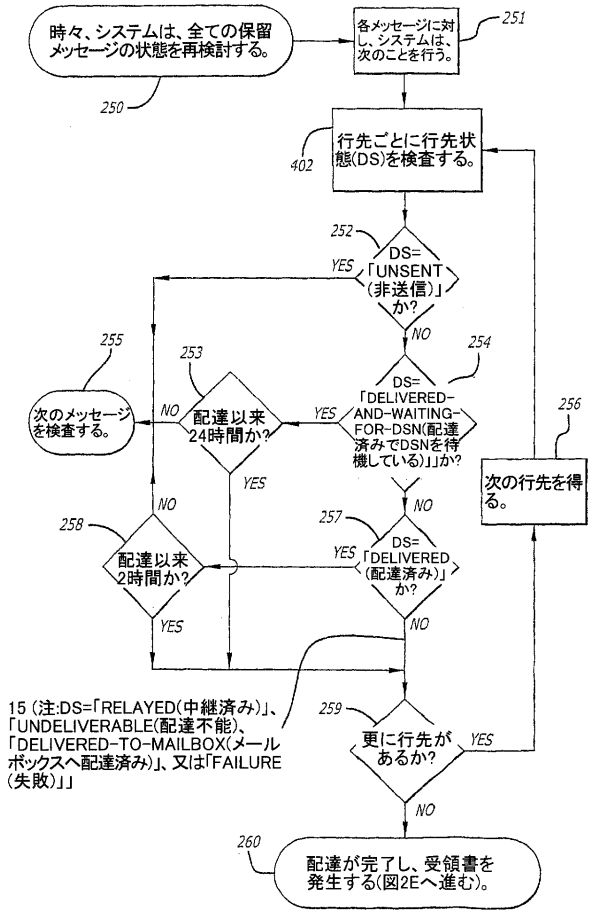
【図２Ｂ－２】



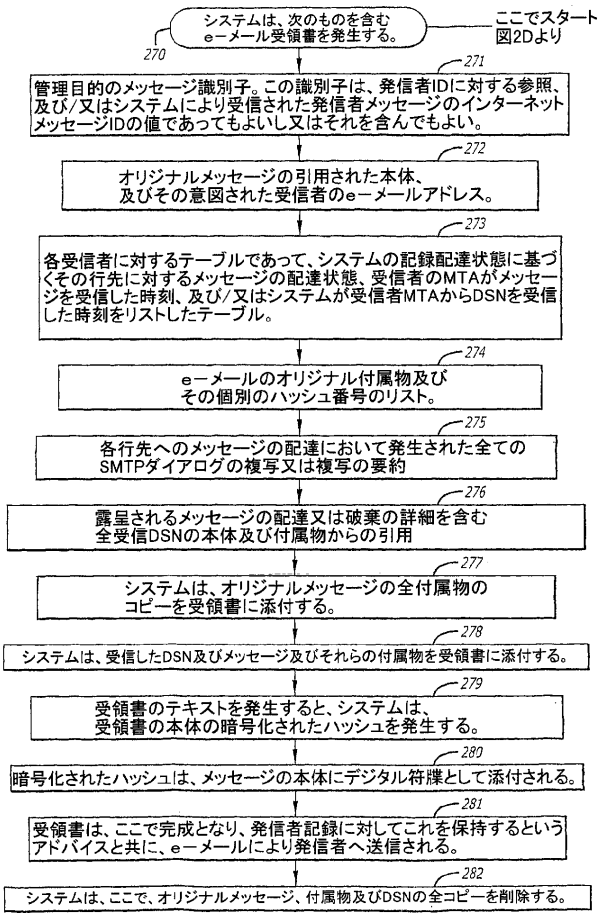
【図２Ｃ】



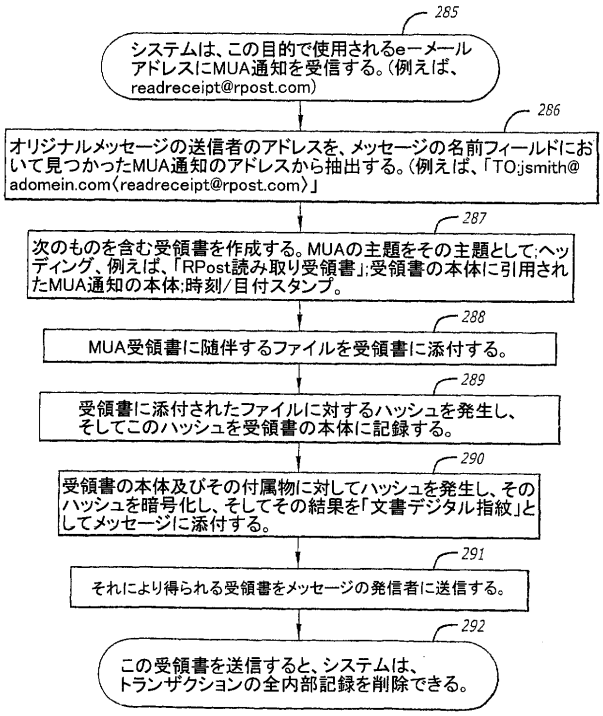
【図２Ｄ】



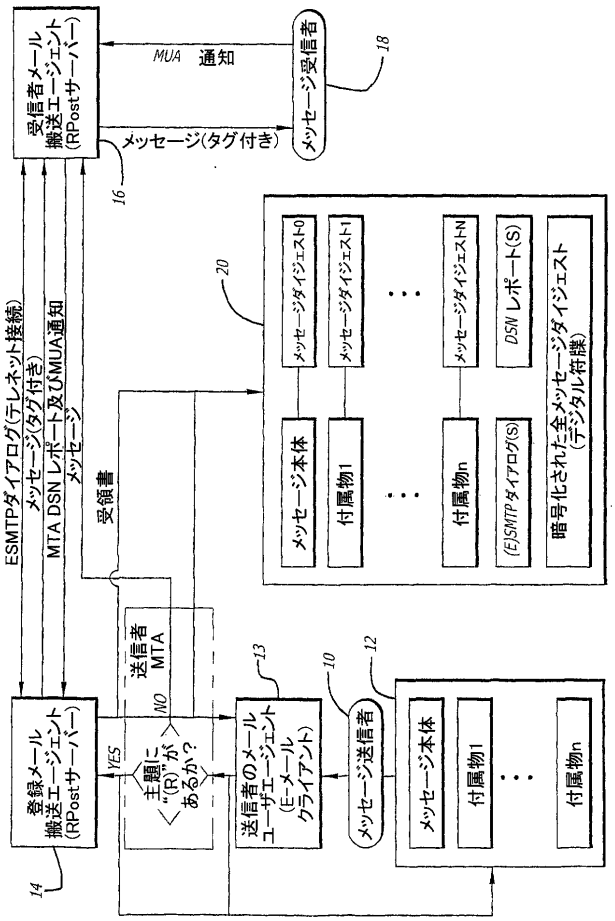
【図２Ｅ】



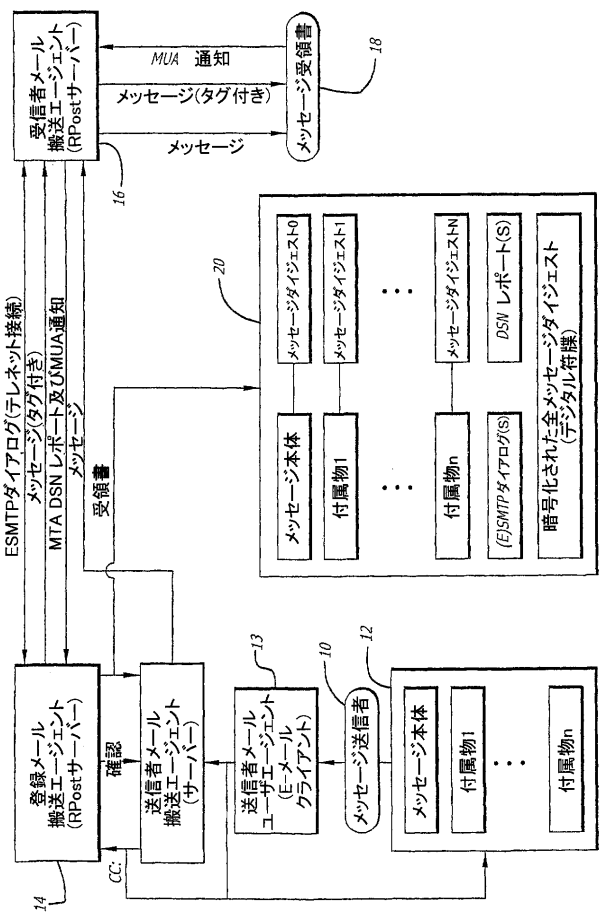
【図２Ｆ】



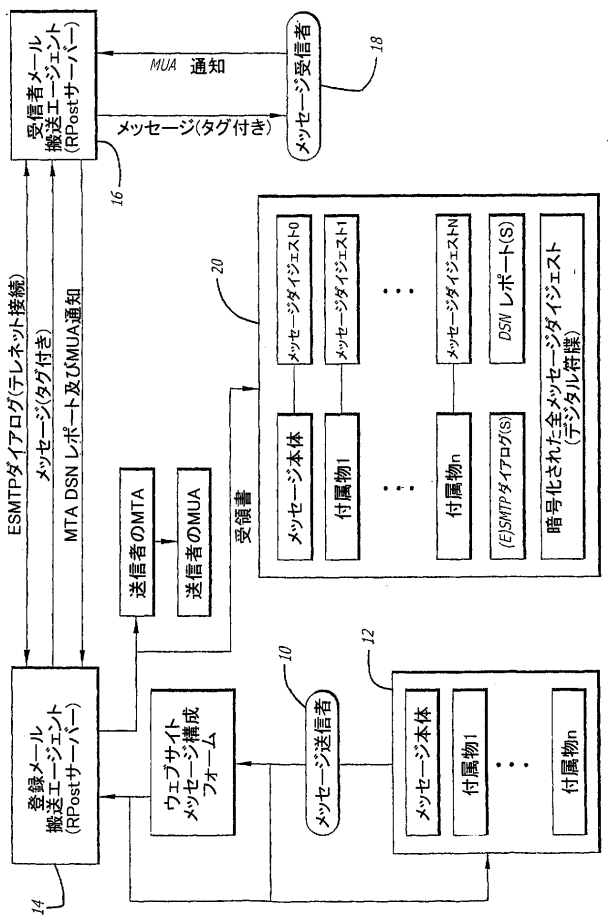
【図３】


受信者メール搬送エージェント(RPostサーバー)
MUA 通知
メッセージ(タグ付き)
メッセージ受信者
ESMTPダイアログ(テレネット接続)
メッセージ(タグ付き)
MTA DSN レポート及びMUA通知
メッセージ
受領書
登録メール搬送エージェント(RPostサーバー)
主題に"(R)"があるか?
YES
NO
送信者MTA
送信者のメールユーザエージェント(E-メールクライアント)
メッセージ送信者
メッセージ本体
付属物1
付属物n
メッセージダイジェスト0
メッセージダイジェスト1
メッセージダイジェストN
DSN レポート(S)
(E)SMTPダイアログ(S)
暗号化された全メッセージダイジェスト(デジタル符牒)
16
18
20
10
12
13
14

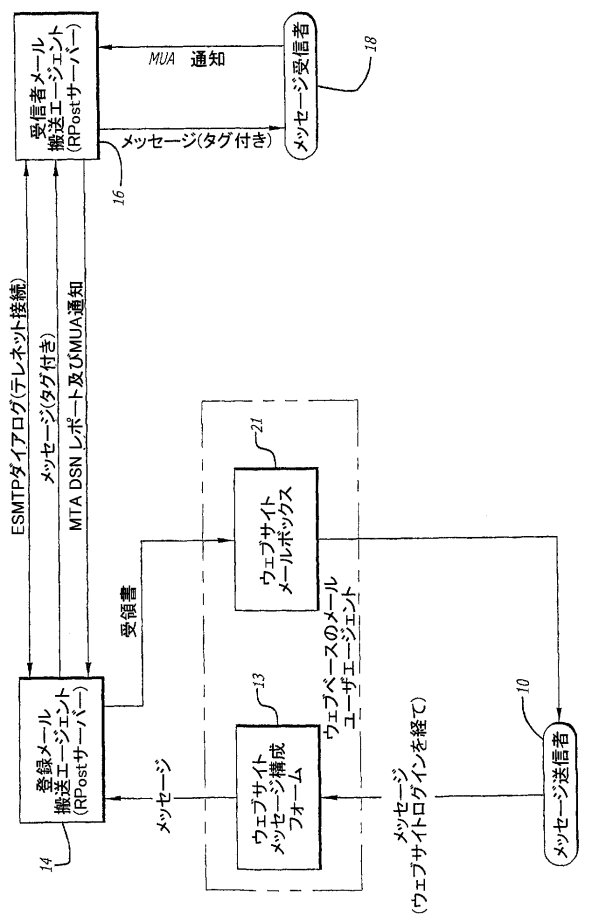
【図４】


受信者メール搬送エージェント(RPostサーバー)
MUA 通知
メッセージ(タグ付き)
メッセージ
メッセージ受領書
ESMTPダイアログ(テレネット接続)
メッセージ(タグ付き)
MTA DSN レポート及びMUA通知
メッセージ
受領書
登録メール搬送エージェント(RPostサーバー)
確認
送信者メール搬送エージェント(サーバー)
送信者メールユーザエージェント(E-メールクライアント)
メッセージ送信者
メッセージ本体
付属物1
付属物n
CC:
メッセージダイジェスト0
メッセージダイジェスト1
メッセージダイジェストN
DSN レポート(S)
(E)SMTPダイアログ(S)
暗号化された全メッセージダイジェスト(デジタル符牒)
16
18
20
10
12
13
14

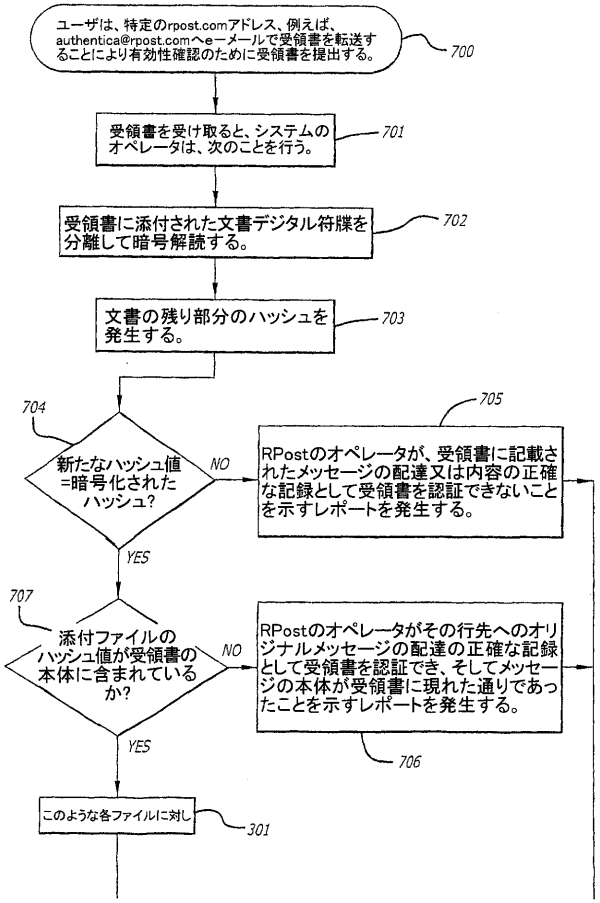
【図５】


受信者メール搬送エージェント(RPostサーバー)
MUA 通知
メッセージ(タグ付き)
メッセージ受信者
ESMTPダイアログ(テレネット接続)
メッセージ(タグ付き)
MTA DSN レポート及びMUA通知
受領書
送信者のMTA
送信者のMUA
登録メール搬送エージェント(RPostサーバー)
ウェブサイトメッセージ構成フォーム
メッセージ送信者
メッセージ本体
付属物1
付属物n
メッセージダイジェスト0
メッセージダイジェスト1
メッセージダイジェストN
DSN レポート(S)
(E)SMTPダイアログ(S)
暗号化された全メッセージダイジェスト(デジタル符牒)
16
18
20
10
12
14

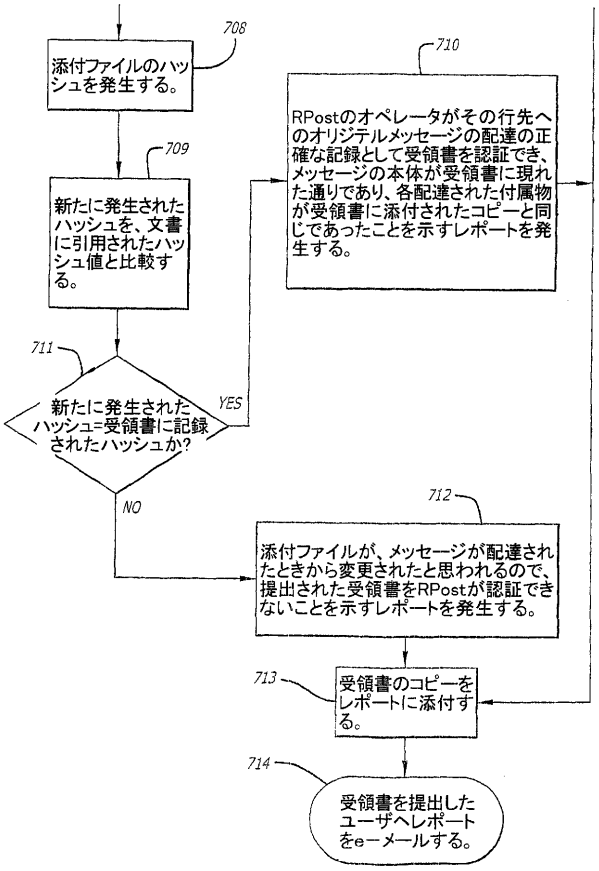
【図６】


受信者メール搬送エージェント(RPostサーバー)
MUA 通知
メッセージ(タグ付き)
メッセージ受信者
ESMTPダイアログ(テレネット接続)
メッセージ(タグ付き)
MTA DSN レポート及びMUA通知
受領書
登録メール搬送エージェント(RPostサーバー)
ウェブサイトメッセージ構成フォーム
ウェブサイトメールボックス
ウェブベースのメールユーザエージェント
メッセージ
メッセージ(ウェブサイトログインを経て)
メッセージ送信者
16
18
21
10
13
14

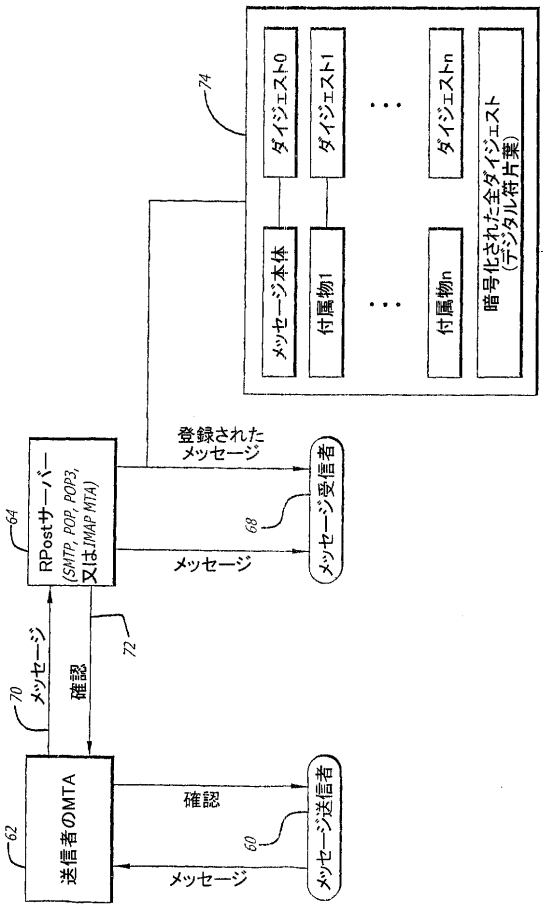
【図７ａ】


ユーザは、特定のrpost.comアドレス、例えば、authentica@rpost.comへe－メールで受領書を転送することにより有効性確認のために受領書を提出する。
700
受領書を受け取ると、システムのオペレータは、次のことを行う。
701
受領書に添付された文書デジタル符牒を分離して暗号解読する。
702
文書の残り部分のハッシュを発生する。
703
704
新たなハッシュ値=暗号化されたハッシュ?
NO
705
RPostのオペレータが、受領書に記載されたメッセージの配達又は内容の正確な記録として受領書を認証できないことを示すレポートを発生する。
YES
707
添付ファイルのハッシュ値が受領書の本体に含まれているか?
NO
RPostのオペレータがその行先へのオリジナルメッセージの配達の正確な記録として受領書を認証でき、そしてメッセージの本体が受領書に現れた通りであったことを示すレポートを発生する。
706
YES
このような各ファイルに対し
301

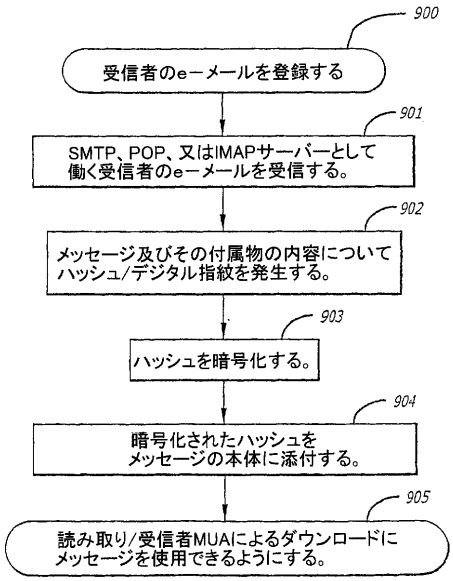
【図７ｂ】


添付ファイルのハッシュを発生する。
708
709
新たに発生されたハッシュを、文書に引用されたハッシュ値と比較する。
710
RPostのオペレータがその行先へのオリジテルメッセージの配達の正確な記録として受領書を認証でき、メッセージの本体が受領書に現れた通りであり、各配達された付属物が受領書に添付されたコピーと同じであったことを示すレポートを発生する。
711
新たに発生されたハッシュ=受領書に記録されたハッシュか?
YES
NO
712
添付ファイルが、メッセージが配達されたときから変更されたと思われるので、提出された受領書をRPostが認証できないことを示すレポートを発生する。
713
受領書のコピーをレポートに添付する。
714
受領書を提出したユーザへレポートをe－メールする。

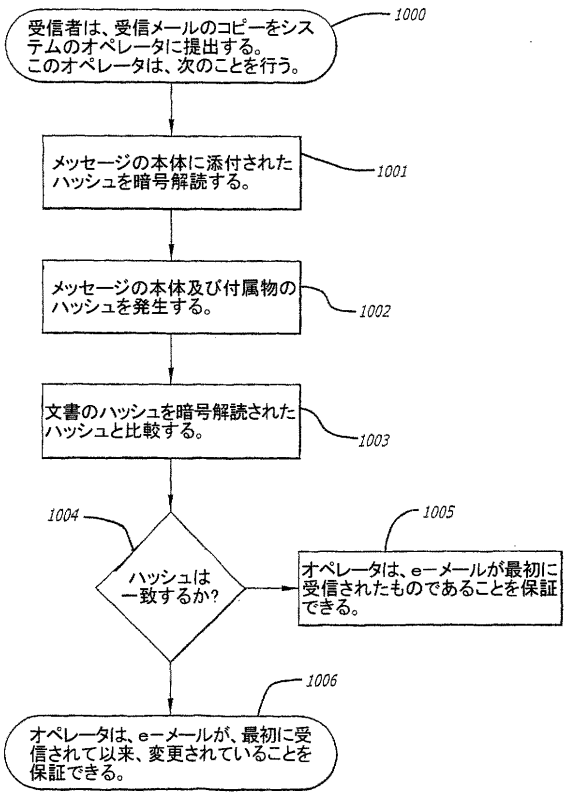
【図８】


74
ダイジェスト0
ダイジェスト1
ダイジェストn
暗号化された全ダイジェスト(デジタル符牒)
メッセージ本体
付属物1
付属物n
登録されたメッセージ
RPostサーバー(SMTP, POP, POP3, 又はIMAP MTA)
64
68
メッセージ受信者
メッセージ
72
確認
70
メッセージ
送信者のMTA
62
確認
60
メッセージ送信者
メッセージ

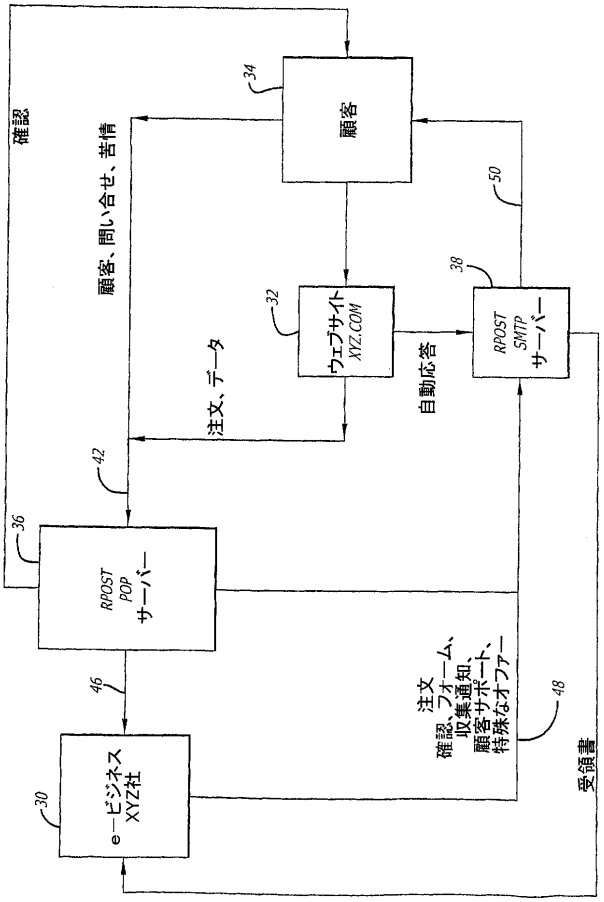
【図９】


900
受信者のe－メールを登録する
901
SMTP、POP、又はIMAPサーバーとして働く受信者のe－メールを受信する。
902
メッセージ及びその付属物の内容についてハッシュ/デジタル指紋を発生する。
903
ハッシュを暗号化する。
904
暗号化されたハッシュをメッセージの本体に添付する。
905
読み取り/受信者MUAによるダウンロードにメッセージを使用できるようにする。

【図１０】


受信者は、受信メールのコピーをシステムのオペレータに提出する。このオペレータは、次のことを行う。
1000
メッセージの本体に添付されたハッシュを暗号解読する。
1001
メッセージの本体及び付属物のハッシュを発生する。
1002
文書のハッシュを暗号解読されたハッシュと比較する。
1003
1004
ハッシュは一致するか?
1005
オペレータは、e－メールが最初に受信されたものであることを保証できる。
1006
オペレータは、e－メールが、最初に受信されて以来、変更されていることを保証できる。

【図１１】


確認
顧客、問い合せ、苦情
注文、データ
自動応答
注文
確認、フォーム、
収集通知、
顧客サポート、
特殊なオファー
受領書
顧客
ウェブサイト
XYZ.COM
RPOST
SMTP
サーバー
RPOST
POP
サーバー
e－ビジネス
XYZ社
34
32
38
50
42
36
46
48
30

フロントページの続き

(74)代理人 100084663
弁理士 箱田 篤
(72)発明者 トムコウ テランス エイ
アメリカ合衆国 カリフォルニア州 ９００１９ ロサンゼルス カーモナ アヴェニュー １３０１

Ｆターム(参考) 5B084 AA01 AA15 AB02 AB03 AB22 AB36 CB04 CB06 CB22
5J104 AA08 JA21 LA03 LA06 NA02 NA37 NA38 PA08
5K030 GA17 HA06 JT02 LD13