(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2005-285116
(P2005-285116A)
(43)公開日　平成17年10月13日(2005.10.13)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 13/00	G06F	13/00	610Q	5K030
H04L 12/58	H04L	12/58	100F	

審査請求 未請求　請求項の数 36　ＯＬ　外国語出願　（全 25 頁）

(21)出願番号　特願2005-82473(P2005-82473)
(22)出願日　平成17年3月22日(2005.3.22)
(31)優先権主張番号　10/806,020
(32)優先日　平成16年3月22日(2004.3.22)
(33)優先権主張国　米国(US)

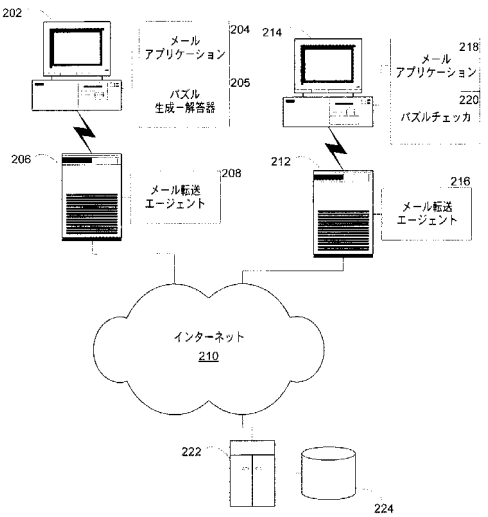
（特許庁注：以下のものは登録商標）
1．ＣＯＭＰＡＣＴＦＬＡＳＨ

(71)出願人　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　アンドリュー　ディー．バイレル
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】大量電子メールメッセージを阻止する暗号パズル消印サービス

(57)【要約】
【課題】　暗号パズルの識別子のデータベースを維持する消印サーバの方法およびシステムを提供すること。
【解決手段】　暗号パズルは、一意の識別子、およびタイムスタンプから作成され、パズルの解答とともに電子メールメッセージに添付される。受信者は、解答が正しく、タイムスタンプが現在であることを確認し、さらに消印サーバに対してパズル識別子についての照会を行う。識別子がデータベースに存在していない場合、受信者は、受信したメッセージが正当であることがわかる。識別子がすでにデータベースにある場合、受信したメッセージは、受信者のコンピュータから自動的に削除することができる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
暗号パズルを含むデジタルオブジェクトの所望の受信者を含むデジタル配信システムで使用するため、識別子に関連付けられる暗号パズルを消印し、少なくとも１つのデータベースに接続する消印サーバであって、
前記受信者のパズルに関連付ける前記識別子を受信するステップと、
前記少なくとも１つのデータベースに対して前記識別子についての照会を行うステップと、
前記照会が失敗すると、エントリを前記少なくとも１つのデータベースに格納することによって前記所望の受信者のパズルを消印するステップと
を実行し、
前記エントリは前記識別子または前記識別子から導出される情報を含むことを特徴とする消印サーバ。
【請求項２】
前記照会が失敗した場合、ＡＣＣＥＰＴ応答を送信するステップをさらに実行することを特徴とする請求項１に記載の消印サーバ。
【請求項３】
前記照会が成功した場合、ＲＥＪＥＣＴ応答を送信するステップをさらに実行することを特徴とする請求項１に記載の消印サーバ。
【請求項４】
前記パズルはさらにタイムスタンプに関連付けられており、前記サーバは前記受信者のパズルに関連付ける前記タイムスタンプを受信するステップをさらに実行し、前記照会が失敗すると前記少なくとも１つのデータベースに格納される前記エントリは、前記タイムスタンプまたは前記タイムスタンプから導出される情報をさらに含むことを特徴とする請求項１に記載の消印サーバ。
【請求項５】
タイムスタンプが閾値範囲外である場合、前記データベースから該タイムスタンプを含むエントリを削除するステップをさらに実行することを特徴とする請求項４に記載の消印サーバ。
【請求項６】
前記少なくとも１つのデータベースに対する照会を行うステップは、前記識別子のハッシュを計算するステップを含むことを特徴とする請求項１に記載の消印サーバ。
【請求項７】
前記識別子は、ピアツーピア分散された検索サービス（ｐｅｅｒ－ｔｏ－ｐｅｅｒ　ｄｉｓｔｒｉｂｕｔｅｄ　ｌｏｏｋｕｐ　ｓｅｒｖｉｃｅ）の値の範囲にさらに対応して前記範囲内の値にハッシュされることを特徴とする請求項６に記載の消印サーバ。
【請求項８】
第２の消印サーバに接続して、前記少なくとも１つのデータベース内のデータを前記第２の消印サーバに提供することを特徴とする請求項１に記載の消印サーバ。
【請求項９】
第２の消印サーバに関連付けられた少なくとも１つのデータベースに対する照会を行う第２の消印サーバに接続していることを特徴とする請求項１に記載の消印サーバ。
【請求項１０】
前記消印サーバおよび前記第２の消印サーバは、ピアツーピアネットワークを介して通信することを特徴とする請求項９に記載の消印サーバ。
【請求項１１】
前記デジタルオブジェクトは、電子メールメッセージであることを特徴とする請求項１に記載の消印サーバ。
【請求項１２】
暗号パズルおよび解答を含むデジタルオブジェクトの所望の受信者を含むデジタル配信

システムで使用するため、識別子およびタイムスタンプに関連付けられた暗号パズルの解答を確認し、少なくとも１つの消印サーバに接続するパズルチェッカであって、
前記パズルに関連付ける前記識別子を前記少なくとも１つの消印サーバに送信するステップと、
前記少なくとも１つの消印サーバからＲＥＪＥＣＴ応答を受信すると、前記デジタルオブジェクトを処理するステップと
を実行することを特徴とするパズルチェッカ。
【請求項１３】
前記デジタルオブジェクトを処理するステップは、前記デジタルオブジェクトを削除するステップを含むことを特徴とする請求項１２に記載のパズルチェッカ。
【請求項１４】
前記デジタルオブジェクトを処理するステップは、該処理後のフィルタリングのために前記デジタルオブジェクトにマーク付けするステップを含むことを特徴とする請求項１２に記載のパズルチェッカ。
【請求項１５】
前記デジタルオブジェクトを処理するステップは、前記デジタルオブジェクトの優先度を変更するステップを含むことを特徴とする請求項１２に記載のパズルチェッカ。
【請求項１６】
前記解答が前記パズルを解くかどうかを確認するステップと、
前記解答が前記パズルを解かない場合、前記デジタルオブジェクトを処理するステップと
をさらに実行することを特徴とする請求項１２に記載のパズルチェッカ。
【請求項１７】
前記タイムスタンプが閾値範囲内かどうかを確認するステップと、
前記タイムスタンプが前記閾値範囲外である場合、前記デジタルオブジェクトを処理するステップと
をさらに実行することを特徴とする請求項１２に記載のパズルチェッカ。
【請求項１８】
前記識別子のハッシュを計算するステップ
をさらに実行し、前記送信するステップは、前記識別子のハッシュに対応する前記少なくとも１つの消印サーバに前記識別子を送信するステップをさらに含む
ことを特徴とする請求項１２に記載のパズルチェッカ。
【請求項１９】
前記パズルチェッカは、前記所望の受信者の場所に存在することを特徴とする請求項１２に記載のパズルチェッカ。
【請求項２０】
前記パズルチェッカは、中間サーバの場所に存在することを特徴とする請求項１２に記載のパズルチェッカ。
【請求項２１】
前記中間サーバは、前記少なくとも１つの消印サーバからＲＥＪＥＣＴ応答が受信されない場合にのみ、前記配信するオブジェクトを前記所望の受信者に送信することを特徴とする請求項２０に記載のパズルチェッカ。
【請求項２２】
少なくとも１つの消印サーバに接続するパズルチェッカ、および暗号パズルおよび解答を含むデジタルオブジェクトの所望の受信者を含むデジタル配信システムで使用するため、暗号パズルを生成し、解くパズル生成器であって、
識別子を生成するステップと、
タイムスタンプを生成するステップと、
前記識別子およびタイムスタンプを使用して暗号パズルを生成するステップと、
前記暗号パズルの解答を計算するステップと

を実行し、
前記パズル、解答、タイムスタンプ、および識別子は、該実行により前記デジタルオブジェクトに添付されて前記所望の受信者に配信されることを特徴とするパズル生成器。
【請求項２３】
前記識別子は、疑似ビットの文字列を含むことを特徴とする請求項２２に記載のパズル生成器。
【請求項２４】
前記識別子は、少なくとも１２８ビットの文字列を含むことを特徴とする請求項２２に記載のパズル生成器。
【請求項２５】
前記暗号パズルの解答を計算するステップは、約７秒を超える計算時間を必要とすることを特徴とする請求項２２に記載のパズル生成器。
【請求項２６】
前記デジタルオブジェクトの送信者から要求を受信するステップと、
前記識別子、タイムスタンプ、パズルおよび解答を前記送信者に送信するステップと
をさらに実行することを特徴とする請求項２２に記載のパズル生成器。
【請求項２７】
前記デジタルオブジェクトの前記送信者から支払いを受信するステップ
をさらに実行することを特徴とする請求項２６に記載のパズル生成器。
【請求項２８】
第１の消印サーバに接続する少なくとも１つのデータベース、および暗号パズルを含むデジタルオブジェクトの所望の受信者を含むデジタル配信システムで使用するため、識別子に関連付けられる暗号パズルを消印する方法であって、
前記受信者のパズルに関連付ける前記識別子を受信するステップと、
前記少なくとも１つのデータベースに対して前記識別子についての照会を行うステップと、
前記照会が失敗すると、エントリを前記少なくとも１つのデータベースに格納することによって前記所望の受信者のパズルを消印するステップと
を含み、前記エントリは前記識別子または前記識別子から導出される情報を含む
ことを特徴とする方法。
【請求項２９】
前記パズルは、さらにタイムスタンプに関連付けられており、前記方法は、前記受信者のパズルに関連付ける前記タイムスタンプを受信するステップをさらに含み、前記照会が失敗すると前記少なくとも１つのデータベースに格納される前記エントリは、前記タイムスタンプまたは前記タイムスタンプから導出される情報をさらに含むことを特徴とする請求項２８に記載の方法。
【請求項３０】
タイムスタンプが閾値範囲外である場合、前記データベースから該タイムスタンプを含むエントリを削除するステップをさらに含むことを特徴とする請求項２９に記載の方法。
【請求項３１】
前記少なくとも１つのデータベース内のデータを第２の消印サーバに提供するステップをさらに含むことを特徴とする請求項２８に記載の方法。
【請求項３２】
第２の消印サーバに関連付けられた前記少なくとも１つのデータベースに対する照会を行うステップをさらに含むことを特徴とする請求項２８に記載の方法。
【請求項３３】
前記第１の消印サーバおよび前記第２の消印サーバは、ピアツーピアネットワークを介して通信することを特徴とする請求項３２に記載の方法。
【請求項３４】
前記第１の消印サーバは、分散されたハッシュテーブルの値の範囲に対応し、前記識別

子は前記範囲内の値にハッシュされることを特徴とする請求項２８に記載の方法。
【請求項３５】
前記デジタルオブジェクトは、電子メールメッセージであることを特徴とする請求項２８に記載の方法。
【請求項３６】
第１の消印サーバに接続する少なくとも１つのデータベース、および暗号パズルを含むデジタルオブジェクトの所望の受信者を含むデジタル配信システムで使用するため、識別子に関連付けられた暗号パズルの消印を可能にするコンピュータ実行可能命令を含むコンピュータ読取可能な媒体であって、前記コンピュータ実行可能命令は、
前記受信者のパズルに関連付ける前記識別子を受信するステップと、
前記少なくとも１つのデータベースに対して前記識別子についての照会を行うステップと、
前記照会が失敗すると、エントリを前記少なくとも１つのデータベースに格納することによって前記所望の受信者のパズルを消印するステップと
を実行し、
前記エントリは、前記識別子または前記識別子から導出される情報を含むことを特徴とするコンピュータ読取可能な媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に分散コンピューティングの分野に関し、より詳細には、インターネットなどのコンピュータネットワークを介して要求されていない電子メッセージを大量に送信するなど、求められていない動作を低減するシステムおよび方法に関する。
【背景技術】
【０００２】
電子メッセージング、特にインターネットを介して運ばれる電子メール（Ｅメール）は、多くの個人および組織にとって好ましい通信方法になってきている。しかし残念なことに、Ｅメールの受信者は、次第に、要求されていない不要な大量のメール送信を受けるようになってきた。インターネットベースの商取引が進展するにつれて、増え続ける多種多様な電子取引者は、拡大を続けるＥメール受信者の市場に対し、要求されていないメールを繰り返し送信して、各自の製品およびサービスの宣伝を行なっているのである。例えば、インターネットユーザが様々なＷｅｂサイトを閲覧する際に何の問題もないように見える閲覧者情報の要求に応答して単にＥメールアドレスを提供しただけで、後に要求していないメールを受け取って、電子配布先リストに含まれてしまったことがわかり不快になることがよくある。これは、ユーザエクスペリエンスに悪影響を与え、仕事場でこうした不要なＥメールや「スパム」を受信する場合にはユーザの生産性が減るおそれがある。
【０００３】
受信者は、自分が電子メーリングリストに含まれていることがわかっても、１度登録されると、仮にそのアドレスをメーリングリストから削除することができるとしても、簡単にはできないため、要求していないメールをその受信者が引き続き受け取ることを効果的に保証することになってしまう。これは、単に送信者がメッセージの受信者がそのメッセージの送信者を特定できないようにしている（例えばプロキシサーバを介してメールを送信することによって）ことから、受信者が配布先リストから削除してもらおうと送信者と連絡をとることができないため、またはその送信者が受信者から以前に受信したそのような削除の要求すべてを単に無視するために起こる。
【０００４】
要求していない一般の郵便物を１年に満たない間に、１人で何百または何千も受け取ることも確かにある。さらに、電子配布先リストを簡単に交換することができ、かなり容易におよびわずかな費用でＥメールメッセージを非常に大量のアドレス全体に配布することができることを考慮すると、単一のＥメールアドレスでもいくつかの配布先リストに含ま

れただけで、要求していないＥメールメッセージをきわめて短い期間の間にかなり大量に受け取ることになることが予想される。さらに、要求していないＥメールメッセージの多くは有害ではないが、とりわけポルノ関連、激高させる題材、罵倒的な題材などにより受信者はかなり不快な思いをすることとなる。一部のもの（ウィルス）は、コンピュータに有害でさえある。こうした要求していないすべてのメッセージは、まとめていわゆる「ジャンク」メールまたは「スパム」の一部となる。

【０００５】

ジャンクＥメール問題に対処するためにＥメールメッセージにデジタル「切手」を必ず添付する方法が提案されている。より一般的には、これらの切手は「作業の証明（ｐｒｏｏｆ－ｏｆ－ｗｏｒｋ）」を構成することができる。基本的な概念は、次のように要約することができる。送信者がＥメールを目的の受信者に送信するときはいつでも、デジタル切手が生成される。物理的な切手とは異なり、送信者はお金を費やすのではなく、代わりにパズルを解くことによってＣＰＵサイクルまたは他のコンピュータシステムリソースを費やし、その解答が切手となる。Ｅメールに切手が必要となるなら、大量のＥメールを出す経済的利点が損なわれるという論理である。単一のデジタル切手では、作成は難しくなく、おそらく数秒の計算時間を要するだけである。しかし、大量のＥメールの送信者は、何千または何十万、あるいはそれ以上のメッセージを非常に迅速に送信することをＥメールに期待しているが、メッセージごとに切手を計算する必要がでてきて、その速度が落ち、ＣＰＵリソースが消費されることとなる。このようにスパム処理をより高価なものにすることにより、スパムの発信者が活動を行うのを阻止するのである。というのは、こうした方式では、各受信者への負担はとるに足らないが、大量Ｅメールの送信者は、大量メールを送信するために実際の費用を払ってかなりの計算リソースを費やさなければならないからである。電子的な切手をＥメールに貼る別の利点は、スパムをフィルタにかけて取り除くキーとして使用することもできることである。容易に検出でき、検証できる切手を追加することによって、ユーザは、この切手が付いていないＥメールをフィルタにかけて取り除くことができることになる。

【０００６】

一部の既知のデジタル切手システムでは、切手は暗号パズルおよび解答の形をとる。パズルは、解くのがほどほどに難しく（すなわちごくわずかといえる量を少し超える程度の時間および演算能力が必要なだけである）、しかしいったん解答を手にいれると、一般的な数学の問題のように確認は簡単である。一部の研究者は、暗号パズルをデジタル切手として使用するため、所望の質を有する数学関数、およびプロトコルおよびシステムを研究している。これらの研究者には、不要なＥメールに対する抑止力として暗号パズルの使用を提案したＤｗｏｒｋおよびＮａｏｒ（非特許文献１）、メーリングリストの保護、およびサービス妨害攻撃の停止に使用するハッシュキャッシュを後に提案したＡｄａｍ　Ｂａｃｋ（http://cypherspace.org/～adam/hashcash/から入手可能な非特許文献２を参照）、特に有用な数学関数を研究したＡｂａｄｉら（非特許文献３）、および同様の研究を行ったＤｗｏｒｋら（非特許文献４）などがいる。上記の参考文献は、そのどんな部分も排除することなく、示唆するすべてについてその全体を参照により本明細書に組み込む。

【０００７】

【非特許文献１】"Pricing via Processing or Combatting Junk Mail," Lecture Notes in Computer Science 740 (Proceedings of CRYPTO '92), 1993, pp. 137-147
【非特許文献２】"Hashcash - a Denial of Service Counter-Measure, August 2002
【非特許文献３】"Moderately Hard, memory-bound Functions", Proceedings of the 10th Annual Network and Distributed System Security Symposium, February 2003
【非特許文献４】"On Memory-Bound Functions for Fighting Spam", Proceedings of the 23rd Annual International Cryptology Conference (CRYPTO 2003), August 2003
【非特許文献５】M. Abadi, A. Birrell, M. Burrows, F. Dabek, and T. Wobber, in Bankable Postage for Network Services, Proceedings of the 8th Asian Computing Science Conference, Mumbai, India, December 2003

【非特許文献６】Stoica et al., "Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications", Proceedings of the 2001 conference on applications, technologies, architectures, and protocols for computer communications. 2001, pp. 149-160
【非特許文献７】L. von Ahn, Manuel Blum, and John Langford, in Telling Humans and Computers Apart, Communications of the ACM, Feb 2004, Vol. 47. No. 2

【発明の開示】
【発明が解決しようとする課題】
【０００８】
デジタル切手に関する１つの問題は、１つのＥメールメッセージの切手として使用される暗号パズル－解答を第２のＥメールメッセージの切手として再利用することができないようにするということである。パズル－解答を再利用することができると、悪意のあるＥメールの送信者が１つのパズル－解答をコピーして複数のメッセージに使用することができ、受信者はこれらのメッセージが不当であることを知る方法がないことになる。上記のＤｗｏｒｋ－Ｎａｏｒのものやハッシュキャッシュなど、一部の既存のデジタル切手システムは、パズルをメッセージ自体の数学関数となるように要求することによってこの問題に対処している。このようにすることによって、こうしたシステムでのパズル－解答は一意にメッセージに結合される。これらのシステムにより、パズル－解答が再利用されるのを防ぐことができるが、事前にパズル－解答が作成される前にメッセージがすでに作成されていなければならない。
【０００９】
他の既知のデジタル切手システムは、「チケットサーバ」の使用によってこの制限に対処する。チケットサーバは、暗号パズルをオフラインで生成する中央サーバである。Ｅメールの送信者は、例えば暗号パズルを解くことによってチケットを取得する。チケットは、ある受信者向けのＥメールメッセージに添付され、次いでその受信者は、中央チケットサーバに問い合わせることによってチケットの妥当性を確認する。チケットサーバは、同じチケットを複数回使用できないようにするために、使用されたチケットに「消印」を施す。これらのシステムでは、メッセージの作成前に電子切手を作成することはできるが、Ｅメールの送信者および受信者が同じ中央サーバを使用し、信頼している必要がある。こうしたチケットサーバシステムは、非特許文献５に記載されており、そのどんな部分も排除することなく、示唆するすべてについてその全体を参照により本明細書に組み込む。
【課題を解決するための手段】
【００１０】
本発明の実施態様は、大量電子メールメッセージの送信を阻止するために、消印サーバ（ｃａｎｃｅｌｌａｔｉｏｎ　ｓｅｒｖｅｒ）を使用して暗号パズルのチェックを容易にする方法およびシステムを提供する。実施態様の例は、Ｅメールの送信者が無作為に生成された暗号パズルの形の「切手」を添付する必要があるシステムに関する。その数学的な性質のため、各パズルを生成するのにかなりの計算リソースが必要とされる。したがって、配信に切手が必要な場合、Ｅメールを大量の受信者に送信することは、計算上高価である。システムを実行するために、本発明の実施形態は、消印サーバを使用して、「切手」が必ず「消印され（ｃａｎｃｅｌｌｅｄ）」、決して再利用されないようにする。切手は、Ｅメールメッセージを作成する前に生成することができ、送信者は、チケットまたは任意の情報を消印サーバまたは他の任意の中央サーバから取得する必要がない。
【００１１】
一般に、本発明の実施態様では、暗号パズルは、一意の識別子およびタイムスタンプから作成され、パズルの解答とともに電子メールメッセージなどのデジタルオブジェクトに添付される。オブジェクトの受信者は、解答が正しく、タイムスタンプが現在であり、タイムスタンプおよび識別子がパズルに対応していることを確認する。さらに受信者は、消印サーバに対して、パズルの識別子およびタイムスタンプについての照会を行う。識別子は、本当に一意である場合、データベースには存在しておらず、受信者は、受信したオブ

ジェクトが正当なものであることがわかる。識別子が一意でない場合、データベースにすでに存在している可能性があり、受信したオブジェクトを受信者のコンピュータから自動的に削除することができる。個々のメッセージ送信者が暗号パズルを別々に生成し、都合の良いときにパズルを解き、その後それを電子メールメッセージに添付することができるので、本発明は、従来技術に勝る利点を提供する。従来のシステムとは異なり、パズルは添付のメッセージから独立しており、信頼できる独立したソースによってパズルを生成する必要はない。

【００１２】

さらに、一部の実施態様では、複数の消印サーバが使用される。複数の消印サーバは独立して動作し、互いに照会を行い、または消印を施された識別子のデータベースを共有する。

【００１３】

本発明の一態様において、暗号パズルを含むデジタルオブジェクトの目的の受信者を含むデジタル配信システムで使用する識別子に関連付けられた暗号パズルを消印する消印サーバであって、消印サーバは少なくとも１つのデータベースに接続しており、受信者のパズルに関連付けられた識別子を受信するステップと、少なくとも１つのデータベースに対して識別子についての照会を行うステップと、照会が失敗すると、エントリを少なくとも１つのデータベースに格納することによって受信者のパズルを消印するステップとを実行し、エントリは識別子または識別子から導出される情報を含む消印サーバが提供される。一実施態様において、パズルはさらにタイムスタンプに関連付けられており、サーバは受信者のパズルに関連付けられたタイムスタンプを受信するステップをさらに実行し、少なくとも１つのデータベースに格納されるエントリは、照会が失敗すると、タイムスタンプまたはタイムスタンプから導出される情報をさらに含む。別の実施態様において、消印サーバは、少なくとも１つのデータベース内のデータを第２の消印サーバに提供する第２の消印サーバに接続している。一部の実施態様において、デジタルオブジェクトは電子メールメッセージである。

【００１４】

本発明の別の態様によれば、暗号パズルおよび解答を含むデジタルオブジェクトの目的の受信者を含むデジタル配信システムで使用する識別子およびタイムスタンプに関連付けられた暗号パズルの解答を確認するパズルチェッカであって、パズルチェッカは少なくとも１つの消印サーバに接続されており、パズルに関連付けられた識別子を少なくとも１つの消印サーバに送信するステップと、少なくとも１つの消印サーバからＲＥＪＥＣＴ応答が受信されると、デジタルオブジェクトを削除するステップとを実行するパズルチェッカが提供される。一実施態様において、パズルチェッカは、解答がパズルを解くかどうかを確認するステップと、解答がパズルを解かない場合はデジタルオブジェクトを削除するステップとをさらに実行する。別の実施態様において、パズルチェッカは、タイムスタンプが閾値範囲内にあるかどうかを確認するステップと、タイムスタンプが閾値範囲外にある場合はデジタルオブジェクトを削除するステップとをさらに実行する。あるバージョンにおいて、パズルチェッカは、目的の受信者のところにある。別のバージョンにおいて、パズルチェッカは、中間サーバのところにある。

【００１５】

本発明の別の態様によれば、少なくとも１つの消印サーバに接続するパズルチェッカ、および暗号パズルおよび解答を含むデジタルオブジェクトの目的の受信者を含むデジタル配信システムで使用する暗号パズルを生成し、解くパズル生成器であって、パズル生成器は、識別子を生成するステップと、タイムスタンプを生成するステップと、識別子およびタイムスタンプを使用して暗号パズルを生成するステップと、暗号パズルの解答を計算するステップとを実行し、それによってパズル、解答、タイムスタンプ、および識別子は目的の受信者に配信するデジタルオブジェクトに添付されるパズル生成器が提供される。

【００１６】

本発明の別の態様によれば、第１の消印サーバに接続する少なくとも１つのデータベー

ス、および暗号パズルを含むデジタルオブジェクトの目的の受信者を含むデジタル配信システムで使用する、識別子に関連付けられた暗号パズルを消印する方法であって、受信者のパズルに関連付けられた識別子を受信するステップと、少なくとも１つのデータベースに対して識別子についての照会を行うステップと、照会が失敗すると、エントリを少なくとも１つのデータベースに格納することによって受信者のパズルを消印するステップとを含み、エントリは識別子または識別子から導出される情報を含む方法が提供される。

【００１７】

本発明の別の態様によれば、第１の消印サーバに接続する少なくとも１つのデータベース、および暗号パズルを含むデジタルオブジェクトの目的の受信者を含むデジタル配信システムで使用する、識別子に関連付けられた暗号パズルの消印を容易にするためのコンピュータ実行可能命令を含むコンピュータ読取可能な媒体であって、コンピュータ実行可能命令は、受信者のパズルに関連付けられた識別子を受信するステップと、少なくとも１つのデータベースに対して識別子についての照会を行うステップと、照会が失敗すると、エントリを少なくとも１つのデータベースに格納することによって目的の受信者のパズルを消印するステップとを実行し、エントリは識別子または識別子から導出される情報を含むコンピュータ実行可能命令を含むコンピュータ実行可能命令が提供される。

【００１８】

添付の特許請求の範囲には本発明の特徴を詳しく記載しているが、以下の詳細な説明を添付の図面と併せ読めば、本発明およびその利点を最もよく理解できよう。

【発明を実施するための最良の形態】

【００１９】

次に、いくつかの実施形態を参照して暗号パズルの消印サービスをサポートする方法およびシステムについて説明するが、本発明の方法およびシステムは、示した実施形態に限定されるものではない。さらに、本明細書に記載した方法およびシステムは単に例にすぎず、本発明の意図および範囲から逸脱することなく変更を加えることができることを当業者であれば容易に理解されよう。

【００２０】

本発明は、以下の詳細な説明を添付の図面と併せ読めば、より完全に理解できる。この説明では、同様の番号は、本発明の様々な実施形態の中の同様の要素を示している。本発明は、適したコンピューティング環境で実施されるものとして示されている。必須ではないが、本発明を、パーソナルコンピュータによって実行されるプロシージャなどのコンピュータ実行可能命令の一般的な文脈で説明する。一般にプロシージャは、特定のタスクを実行する、または特定の抽象データ型を実装するプログラムモジュール、ルーチン、関数、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。さらに、本発明は、ハンドヘルド装置、マルチプロセッサシステム、マイクロプロセッサベースまたはプログラム可能家庭用電化製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータなどを含む他のコンピュータシステム構成で実施できることを当分野の技術者であれば理解できよう。また、本発明は、タスクが通信ネットワークによってリンクされているリモート処理装置によって実行される分散コンピューティング環境でも実施することができる。分散コンピューティング環境では、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に置くことができる。コンピュータシステムという用語は、分散コンピューティング環境に見られるものなど、コンピュータのシステムを指すために使用され得る。

【００２１】

図１は、本発明を実施するのに適したコンピューティングシステム環境１００の例を示している。コンピューティングシステム環境１００は、適したコンピューティング環境の一例にすぎず、本発明の使用または機能の範囲に関する限定を示唆するものではない。また、コンピューティング環境１００を、動作環境１００の例に示した構成要素のいずれか１つ、またはその組合せに関連する依存性または必要条件を有しているものと解釈すべきではない。本発明の一実施形態は、動作環境１００の例に示した各構成要素を含むが、本

発明の別のより一般的な実施形態は、不必要な構成要素、例えばネットワーク通信に必要なもの以外の入力／出力装置を除いている。

【００２２】

図１を参照すると、本発明を実施するシステムの例は、汎用コンピューティング装置をコンピュータ１１０の形で含んでいる。コンピュータ１１０の構成要素は、それだけには限定されないが、処理ユニット１２０、システムメモリ１３０、およびシステムメモリを含む様々なシステム構成要素を処理ユニット１２０に結合するシステムバス１２１を含み得る。システムバス１２１は、様々なバスアーキテクチャのうちの任意のものを使用する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どんなものでもよい。こうしたアーキテクチャには、それだけには限定されないが一例として、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、拡張ＩＳＡ（ＥＩＳＡ）バス、ビデオ電子装置規格化協会（ＶＥＳＡ）ローカルバス、およびメザニンバスとしても知られている周辺部品相互接続（ＰＣＩ）バスなどがある。

【００２３】

コンピュータ１１０は、一般に様々なコンピュータ読取可能な媒体を含む。コンピュータ読取可能な媒体は、コンピュータ１１０からアクセスできる使用可能な任意の媒体とすることができ、揮発性および不揮発性媒体、取外式および固定式の媒体を含む。コンピュータ読取可能な媒体は、それだけには限定されないが一例として、コンピュータ記憶媒体および通信媒体を含み得る。コンピュータ記憶媒体には、コンピュータ読取可能な命令、データ構造、プログラムモジュール、他のデータなど、情報を記憶するための任意の方法または技術で実施される揮発性および不揮発性の取外式および固定式の媒体がある。コンピュータ記憶媒体には、それだけには限定されないが、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）または他の光ディスク記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置または他の磁気記憶装置、または所望の情報の格納に使用でき、コンピュータ１１０からアクセスできる他の任意の媒体などがある。通信媒体は一般に、コンピュータ読取可能な命令、データ構造、プログラムモジュール、または他のデータを搬送波または他の移送機構などの変調されたデータ信号に組み込む。これには任意の情報配送媒体がある。「変調されたデータ信号」という用語は、信号に情報を符号化するように１つまたは複数のその特性が設定または変更された信号を意味する。通信媒体には、それだけには限定されないが一例として、有線ネットワーク、直接配線された接続などの有線媒体、および音響、ＲＦ、赤外線、その他の無線媒体などの無線媒体がある。また、上記のどんな組合せでもコンピュータ読取可能な媒体の範囲内に含まれる。

【００２４】

システムメモリ１３０は、読み取り専用メモリ（ＲＯＭ）１３１やランダムアクセスメモリ（ＲＡＭ）１３２など、揮発性および／または不揮発性メモリの形のコンピュータ記憶媒体を含む。基本入出力システム１３３（ＢＩＯＳ）は、例えば起動中など、コンピュータ１１０内の要素間での情報の転送を助ける基本ルーチンを含み、一般にＲＯＭ１３１に格納されている。ＲＡＭ１３２は一般に、処理ユニット１２０から直接アクセス可能な、かつ／または処理ユニット１２０が現在処理しているデータおよび／またはプログラムモジュールを含む。図１は、それだけには限定されないが一例として、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７を示している。

【００２５】

コンピュータ１１０は、他の取外式／固定式、揮発性／不揮発性コンピュータ記憶媒体を含むこともできる。一例にすぎないが、図１は、固定式不揮発性磁気媒体から読み取り、あるいはそこに書き込むハードディスクドライブ１４１、取外式不揮発性磁気ディスク１５２から読み取り、あるいはそこに書き込む磁気ディスクドライブ１５１、およびＣＤ－ＲＯＭや他の光媒体など、取外式不揮発性光ディスク１５６から読み取り、あるいはそ

こに書き込む光ディスクドライブ１５５を示している。動作環境の例で使用できる他の取外式／固定式、揮発性／不揮発性コンピュータ記憶媒体には、それだけには限定されないが、磁気テープカセット、フラッシュメモリカード、デジタル多用途ディスク、デジタルビデオテープ、半導体ＲＡＭ、半導体ＲＯＭ、スマートカード、ＳｅｃｕｒｅＤｉｇｉｔａｌカード、ＳｍａｒｔＭｅｄｉａ（登録商標）カード、ＣｏｍｐａｃｔＦｌａｓｈカードなどがある。ハードディスクドライブ１４１は一般に、インターフェース１４０などの固定式メモリインターフェースを介してシステムバス１２１に接続され、磁気ディスクドライブ１５１および光ディスクドライブ１５５は一般に、インターフェース１５０などの取外式メモリインターフェースによってシステムバス１２１に接続される。

【００２６】

上述し、図１に示したドライブおよびその関連のコンピュータ記憶媒体は、コンピュータ読取可能な命令、データ構造、プログラムモジュール、およびコンピュータ１１０の他のデータの記憶域を提供する。図１では例えば、ハードディスクドライブ１４１は、オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７を記憶するものとして示されている。これらの構成要素は、オペレーティングシステム１３４、アプリケーションプログラム１３５、他のプログラムモジュール１３６、およびプログラムデータ１３７と同じであっても、異なっていてもよいことに留意されたい。オペレーティングシステム１４４、アプリケーションプログラム１４５、他のプログラムモジュール１４６、およびプログラムデータ１４７は少なくとも異なるコピーであることを示すために、ここではそれらに異なる番号を付している。ユーザは、タブレットまたは電子デジタイザ１６４などの入力装置、マイクロフォン１６３、キーボード１６２、および一般にマウス、トラックボール、またはタッチパッドと呼ばれるポインティング装置１６１などの入力装置を介してコマンドおよび情報をコンピュータ１１０に入力することができる。他の入力装置（図示せず）には、ジョイスティック、ゲームパッド、衛星パラボラアンテナ、スキャナなどがある。これらおよび他の入力装置は、しばしばシステムバスに結合されているユーザ入力インターフェース１６０を介して処理ユニット１２０に接続されるが、パラレルポート、ゲームポート、ユニバーサルシリアルバス（ＵＳＢ）など他のインターフェースおよびバス構造で接続してもよい。モニタ１９１または他のタイプの表示装置もまた、ビデオインターフェース１９０などのインターフェースを介してシステムバス１２１に接続される。モニタ１９１は、タッチ画面パネルなどに一体化することもできる。モニタおよび／またはタッチ画面パネルは、タブレット型パーソナルコンピュータなど、コンピューティング装置１１０が組み込まれるハウジングに物理的に結合することができることに注意されたい。さらに、コンピューティング装置１１０などのコンピュータは、出力周辺インターフェース１９４などを介して接続できるスピーカ１９７、プリンタ１９６などの他の周辺出力装置を含むこともできる。

【００２７】

コンピュータ１１０は、リモートコンピュータ１８０など１つまたは複数のリモートコンピュータへの論理接続を使用してネットワーク式環境で動作することができる。リモートコンピュータ１８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、ピア装置、または他の一般のネットワークノードでよく、一般にコンピュータ１１０に関連して上述した多くまたはすべての要素を含むが、図１にはメモリ記憶装置１８１のみを示している。図１に示した論理接続は、ローカルエリアネットワーク（ＬＡＮ）１７１および広域ネットワーク（ＷＡＮ）１７３を含むが、他のネットワークを含んでいてもよい。こうしたネットワーキング環境は、オフィス、全社規模のコンピュータネットワーク、イントラネット、およびインターネットではごく一般的である。例えば、本発明では、コンピュータ１１０は、ソースマシンを含むことができ、データはそこから移動され、リモートコンピュータ１８０は宛先マシンを含み得る。しかし、ソースマシンおよび宛先マシンは、ネットワークまたは他の任意の手段によって接続される必要はなく、データは、ソースプラットフォームによって書き込まれ、宛先プラットフォームによって読み取られ

ることができる任意の媒体を解して移動することができる。

【００２８】

ＬＡＮネットワーキング環境で使用する場合、コンピュータ１１０は、ネットワークインターフェースまたはアダプタ１７０を介してＬＡＮ１７１に接続される。あるいは、コンピュータ１１０は、例えば８０２．１１ｂプロトコルで動作する無線ＬＡＮネットワークインターフェースを含み、コンピュータ１１０が物理的接続無しにＬＡＮ１７１に接続することができる。ＷＡＮネットワーキング環境で使用する場合、コンピュータ１１０は一般に、モデム１７２、またはインターネットなどＷＡＮ１７３を介して通信を確立する他の手段を含む。モデム１７２は、内蔵のものでも外付けのものでもよく、ユーザ入力インターフェース１６０または他の適切な機構を介してシステムバス１２１に接続することができる。あるいは、コンピュータ１１０は、例えばＧｅｎｅｒａｌ Ｐａｃｋｅｔ Ｒａｄｉｏ Ｓｅｒｖｉｃｅ（ＧＰＲＳ）を介して動作する無線ＷＡＮネットワークインターフェースを含み、コンピュータ１１０が物理的接続無しにＷＡＮ１７３に接続することができる。ネットワーク式環境では、コンピュータ１１０に関連して示したプログラムモジュール、またはその一部をリモートメモリ記憶装置に格納することができる。図１は、それだけには限定されないが一例として、リモートアプリケーションプログラム１８５をメモリ装置１８１上に存在するものとして示している。図示したネットワーク接続は例であり、コンピュータ間の通信リンクを確立する他の手段を使用してもよいことは理解されよう。さらに、セルラー式電話、ＰＤＡなど、本発明を実施するために、コンピュータ１１０の変形形態を他のシステム例に組み込むことができる。

【００２９】

本発明を組み込むコンピューティング装置は、図１に示したコンピューティング装置に類似していても、または代替の構成を含んでいてもよい。本発明は、様々なネットワーク環境で使用されるコンピューティング装置／マシンに潜在的に組み込まれている。図２を参照すると、本発明を活用することができるネットワーキング環境の簡単な例を示している。この実施形態例において、電子メールメッセージは、Ｍｉｃｒｏｓｏｆｔ Ｏｕｔｌｏｏｋ やＭｉｃｒｏｓｏｆｔ Ｏｕｔｌｏｏｋ Ｅｘｐｒｅｓｓなどのメールアプリケーション２０４を使用して第１のコンピュータ２０２上で作成される。第１のコンピュータ２０２上のパズル生成－解答器（ｐｕｚｚｌｅ ｃｒｅａｔｏｒ－ｓｏｌｖｅｒ）２０５は、タイムスタンプおよびグローバルに一意の識別子を使用して、電子メールメッセージの受信者に送信される暗号パズルを作成し、解く。パズルは、解くのに適度な演算能力を必要とし（例えば市販の最速のコンピュータ上で約数秒の時間を要する）、しかし解答はわずかな演算能力のみで確認することができるパズルのクラスのものが好ましい。こうした暗号パズルは、例えば上記のＤｗｏｒｋおよびＮａｏｒ、ならびにハッシュキャッシュなどでより十分に説明されている。あるいは、パズル生成－解答器は、例えば信頼できる独立したパズル作成サーバなどに遠隔に配置される。この代替の構成において、信頼できる独立した機関は、お金と引き換えに、または顧客の購買意欲を促進するものなどとして予め解かれたパズルを配布する。予め解かれたパズルを配布する方式例は、Ｄｗｏｒｋ－Ｎａｏｒ方式など、落とし戸（ｔｒａｐ-ｄｏｏｒ）を含むパズルのクラスを使用する。

【００３０】

電子メールメッセージ、パズル、および解答はタイムスタンプおよび一意の識別子と結合されて、まとめてパッケージが形成され、これがコンピュータ２０２から、一般にコンピュータ２０２へのインターネットアクセスを提供するインターネットサービスプロバイダ（ＩＳＰ）に配置されているメールサーバ２０６に送信される。メールサーバ２０６は、ＳＭＴＰなどのメール送信プロトコルメールを作動させるメール転送エージェント（ＭＴＡ）２０８を使用し、インターネット２１０を介してパッケージを送信し、パッケージは最終的に、受信者のコンピュータ２１４へのインターネットアクセスを提供するＩＳＰに配置されているメールサーバ２１２に到達する。メールサーバ２１２は、ＩＭＡＰなどのメール配送プロトコルを作動させるＭＴＡ２１６を使用して、受信者のコンピュータ２１４上のメールアプリケーション２１８にパッケージを配信する。メールアプリケーショ

ン２１４は、パッケージを開き、パズルチェッカ２２０を使用して、含まれている解答が本当に含まれているパズルを解くことを確認し、またパズルが最近生成されたことを保証するためにタイムスタンプが所与の範囲内であることを確認する。パズル生成－解答器によって使用されるタイムスタンプは、粒子が粗く、時間または日の粒度の精度しかないことが好ましい。

【００３１】

受信者側コンピュータ２１４は、消印サーバ２２２を使用することによって、暗号パズルが他のメールメッセージと共同して使用されていないことをさらにチェックする。消印サーバ２２２は、データ記憶装置を保護するため、好ましくはハッシュ値または一意の識別子から導出された他の情報、およびタイムスタンプを格納することによって、データベース２２４に暗号パズルの一意の識別子およびタイムスタンプを格納する。またはこれに替えて、データ構造は、Ｂｌｏｏｍフィルタとともに使用するようにパズルの消印情報を格納する。受信者側コンピュータ２１４は、消印サーバ２２２への認証済みの接続を確立し、受信されたパッケージからの一意の識別子およびタイムスタンプを、インターネット２１０を介して消印サーバ２２２に送信することが好ましい。消印サーバ２２２は、受信者の一意の識別子はデータベース２２４に存在しないことを確認し、受信者のコンピュータ２１４にパズルが有効であることを通知する。次いで消印サーバ２２２は、一意の識別子およびタイムスタンプをデータベース２２４に追加して、将来のメッセージが特定のパズルを使用しないようにする。このように暗号パズルを消印サーバとともに使用することによって、電子メールメッセージの受信者は、そのメッセージがその受信者が受信するように個々に作成されたものであることを確信する。消印サーバ２２２が非常に積極的で、そのデータベース２２４内の大量のユーザの大量のパズルに消印を施す場合、不当なパズル（すなわち再利用されたパズルを含むもの）が検知されないままである確率は小さくなる。

【００３２】

パズル生成－解答器２０５が高い確率でグローバルに一意の識別子を生成する方法は数多くある。例えば、強い乱数ジェネレータ（ｓｔｒｏｎｇ　ｒａｎｄｏｍ　ｎｕｍｂｅｒ　ｇｅｎｅｒａｔｏｒ）が使用可能な場合、パズル生成－解答器２０５は、単に十分な長さの乱数を生成するだけである。またはこれに替えて、無関係な、しかし本来備わっているコンピュータ２０２の特性を使用して、このコンピュータからの識別子の順序が他のどれとも衝突しないことを保証する。例えば、一実施形態において、パズル生成－解答器２０５は、コンピュータ２０２の４８ビットのＥｔｈｅｒｎｅｔ（登録商標）ＭＡＣアドレスと８０個のランダムビットとを連結する。十分に無作為に行なって、正当なジェネレータが作成することができる識別子を攻撃者が推測するのが手に負えないほど難しくなるようにする。

【００３３】

図３ａを参照すると、本発明の一実施形態では、パズル生成－解答器およびパズルチェッカが、メッセージの送信者およびメッセージの受信者の各々のコンピュータのどこに配置されているかが示される。この実施形態において、送信者のコンピュータは、メールアプリケーション３０２およびパズル生成－解答器３０４を実行させる。これらは互いに協力して動作する。一実施形態において、ユーザは、メールアプリケーション３０２を使用してメールメッセージを生成し、例えばメールアプリケーション３０２のユーザインターフェース上の「送信」とラベル付けされたボタンをクリックすることによって「送信」コマンドを実行する。メールアプリケーション３０２は、実際にメッセージを送信する前に、パズル生成－解答器３０４に対して暗号パズルを生成し、解くよう指示する。パズル生成－解答器３０４は、一意の識別子およびタイムスタンプを生成し、それらを使用して暗号パズルを作成して解答する。パズル生成－解答器３０４は、パズル、解答、タイムスタンプ、および一意の識別子をメールアプリケーション３０２に戻す。メールアプリケーション３０２は、パズル、解答、タイムスタンプ、および一意の識別子をメッセージに添付し、そのメッセージを添付ファイル付きで、一般に送信者のＩＳＰに配置されているメー

ル転送エージェント（ＭＴＡ）３０６に送信する。一実施形態において、予め生成されたパズル／解答がすぐに使用可能なように、またメールアプリケーション３０２がメッセージをＭＴＡ３０６に送信するのに最小限の遅延だけで済むように、パズル生成－解答器３０４は、オフラインプロセスでパズルを生成する。

【００３４】

標準の電子メール処理操作によって、メッセージは、送信者のＭＴＡ３０６から受信者のＭＴＡ３０８に発送される。次いでメッセージは、受信者によって作動されるメールアプリケーション３１０にダウンロードされる。受信者のメールアプリケーション３１０は、添付されたパズルが正当であることを確認するようパズルチェッカ３１２に指示する。パズルチェッカ３１２は、添付された解答がパズルを解くことを確認し、またタイムスタンプが最近生成されたことを保証するために所与の範囲内にあることを確認する。次いでパズルチェッカ３１２は、消印サーバ３１４と通信して、パズルが他の電子メールメッセージに使用されていないことを確認する。パズルチェッカ３１２は、メッセージの一意の識別子およびタイムスタンプを消印サーバ３１４に送信し、消印サーバは、そのデータベース３１６内で一意の識別子を探す。識別子がすでにデータベース内に存在している場合、消印サーバ３１４は、パズルが有効ではないことをパズルチェッカ３１２に知らせる。パズルチェッカ３１２は、メールアプリケーション３１０に、関連のメッセージは有効ではなく、したがってそれは大量Ｅメールである可能性があり、削除すべきであることを通知する。このように、メールアプリケーション３１０は、ユーザの介入なしに不当な大量Ｅメールを自動的に削除する。しかし、一意の識別子がデータベース３１６内に存在していない場合、消印サーバ３１４は、パズルチェッカ３１２にパズルが有効であることを知らせるとともに、識別子が将来使用されるのを防ぐために一意の識別子をデータベース３１６に追加する。本発明のこの実施形態では、ＭＴＡ３０６および３０８は、パズル作成－解答作成－確認プロセスを容易にするために、特別な変更をほとんど、またはまったく必要としない。

【００３５】

代替の実施形態を図３ｂを参照すると、パズル生成－解答器３５０は、一般に送信者のＩＳＰにある送信者のメール転送エージェント３５２に配置されている。この構成において、送信者のコンピュータは、メールアプリケーション３５４を実行する。ユーザは、メールアプリケーション３５４を使用してメールメッセージを作成し、例えばメールアプリケーション３５４のユーザインターフェース上の「送信」とラベル付けされたボタンをクリックすることによって「送信」コマンドを実行する。メールアプリケーション３５４は、メッセージを送信者のＭＴＡ３５２に送信する。ＭＴＡは、暗号パズルを生成し、解くようパズル生成－解答器３５０に指示する。パズル生成－解答器３５０は、一意の識別子およびタイムスタンプを生成し、それらを使用して暗号パズルを作成し、次いで解答する。パズル生成－解答器３５０は、パズル、解答、タイムスタンプ、および一意の識別子をＭＴＡ３５２に戻し、ＭＴＡは、パズル、解答、タイムスタンプ、および一意の識別子をメッセージに添付し、ＳＭＴＰなどのメッセージ送信プロトコルに従ってメッセージを送信する。一実施形態において、予め生成されたパズル／解答がすぐに使用可能なように、またＭＴＡ３５２がメッセージを再送信するのに最小限の遅延だけで済むように、パズル生成－解答器３５０は、オフラインプロセスでパズルを生成する。

【００３６】

標準の電子メール処理操作によって、メッセージは、送信者のＭＴＡ３５２から受信者のＭＴＡ３５６に発送される。ＭＴＡ３５６は、添付されたパズルが正当であることを確認するようパズルチェッカ３５８に指示する。パズルチェッカ３５８は、添付された解答がパズルを解き、タイムスタンプが最近の範囲内であることを確認する。次いでパズルチェッカ３５８は、消印サーバ３６０と通信して、パズルが他の電子メールメッセージに使用されていないことを確認する。パズルチェッカ３５８は、メッセージの一意の識別子およびタイムスタンプを消印サーバ３６０に送信し、消印サーバは、そのデータベース３６２内で一意の識別子を探す。識別子がすでにデータベース内に存在している場合、消印サ

ーバ３６０は、パズルが有効ではないことをパズルチェッカ３５８に知らせる。パズルチェッカ３５６は、ＭＴＡ３５６に、関連のメッセージは有効ではなく、したがってそれは大量Ｅメールである可能性があり、削除すべきであることを通知する。このように、ＭＴＡ３５６は、受信者によって受信される前にも不当な大量Ｅメールを自動的に削除する。しかし、一意の識別子がデータベース３６２内に存在していない場合、消印サーバ３６０は、パズルチェッカ３５８にパズルは有効であることを知らせると同時に、識別子の将来の使用を防ぐために一意の識別子をデータベース３６２に追加する。ＭＴＡ３５６は、パズルが有効であることの確認をパズルチェッカ３５８から受信し、そのメッセージを受信者のメールアプリケーション３６４に送信する。本発明のこの実施形態では、送信者および受信者のメールアプリケーション３５４および３６４は、パズル作成－解答作成－確認プロセスを容易にするため、特別な変更を必要とせず、ユーザからはわからないプロセスで不当な大量Ｅメールが受信者に届くのを防ぐ。

【００３７】

しかし、本発明は、図３ａおよび３ｂに示すような実施形態に限定されるものではなく、他の組合せが可能である。例えば、代替の実施形態において、パズル生成－解答器は送信者のＭＴＡに配置されており、パズルチェッカは受信者のメールアプリケーションに配置されている。別の実施形態において、パズル生成－解答器は送信者のメールアプリケーションに配置されており、パズルチェッカは受信者のＭＴＡに配置されている。さらに別の実施形態において、パズルチェッカは送信者のＭＴＡと受信者のＭＴＡとの間の中間サーバに配置されており、パズルチェッカがメッセージは正当であると認識した場合は、メッセージを受信者のＭＴＡに転送するだけで済むのである。

【００３８】

一構成例において、消印サービスは、ＭＳＮ、ＡＯＬ、ＥａｒｔｈＬｉｎｋなど大きいＩＳＰで、こうしたＩＳＰにおけるアカウント宛てのメールが対応する消印サービスにそのパズルをチェックさせるように実装される。この構成をとる利点として、確実にそのユーザは不当な大量Ｅメールを受信しないようにすることができる。例えば単一の暗号パズルを使用してｍｓｎ．ｃｏｍの複数の受信者にアドレス指定される不当なＥメールは、目的の受信者のうちの１番目のみに配信されることになる。パズルの一意の識別子が消印サーバのデータベースに入力されると、その後照会されても、パズルが無効であり、したがってメッセージは不当であると示されることになる。

【００３９】

一部の実施形態において、パズルチェッカは、複数の消印サーバと通信して、不当なＥメールを検出する可能性を高める。例えば、Ｅメールが同じ暗号パズルを使用して異なる２つの受信者ＡおよびＢに送信されると仮定する。２人の受信者が異なる消印サーバを使用する場合、どちらもパズルの無効を検出せず、メッセージは両方の受信者に配信される。しかし受信者Ａがそれ自身の消印サービスに問い合わせるだけでなく、たまたまＢによって使用された消印サービスである第２の消印サービスに問い合わせた場合、（ユーザＢまたは他のパズルの大量の受信者が前もってそこに問い合わせ、パズルの一意の識別子をデータベースに入力したときは）Ａは第２の消印サービスからパズルの無効を検出する。

【００４０】

別の実施形態において、複数の消印サーバは、互いに通信して、データを配布し、および／または共有する。図４に消印サーバの分散システムの一例を示す。調整消印サーバ（ｃｏｏｒｄｉｎａｔｉｎｇ　ｃａｎｃｅｌｌａｔｉｏｎ　ｓｅｒｖｅｒ）４０２は、複数の消印サーバ間でのデータの配布を管理する中央の調整ポイントとして働く。パズルチェッカ４０６が消印サーバ４０４のうちの１つに対して暗号パズルの一意の識別子についての照会を行うと、照会されたサーバ４０４は、識別子をハッシュし、調整サーバ４０２に連絡する。調整サーバ４０２は、例えばハッシュ値の最小位３桁に基づいて、複数の消印サーバ４０４のうちのどれが特定の一意の識別子への責任を持つかを確認する。調整サーバ４０２は、呼び出し側消印サーバ４０４に適切な消印サーバ４０６のアドレスを戻し、呼び出し側消印サーバ４０４は、適切な消印サーバ４０６に対する照会を直接行う。した

がってこの技術および同様の技術を使用すると、識別子の負荷が複数の消印サーバに分散される。

【００４１】

複数の消印サーバを使用する代替の構成は、サーバ間での情報を共有するものである。例えば、あるＩＳＰにある消印サーバは、そのデータベースの内容を第２のＩＳＰにある消印サーバに定期的に転送する。パズルチェッカが第２の消印サーバに対して一意の識別子についての照会を行うと、識別子は単一の照会で両方の消印サーバから有効にデータを検索する。したがってこの構成は、複数の消印サーバのチェックに必要な照会の回数を低減させる。こうした構成は、参加している消印サーバがＨｏｔｍａｉｌやＡＯＬなど、普及しているＩＳＰおよびメール経路設定業者（ｍａｉｌ　ｒｏｕｔｉｎｇ　ａｇｅｎｃｙ）に関連付けられた場合に特に有用である。

【００４２】

複数の消印サーバを使用する同様の構成は、ピアツーピア（Ｐ２Ｐ）ネットワークとして構成される。消印サーバのＰ２Ｐネットワークは、中央編成機関（ｃｅｎｔｒａｌ　ｏｒｇａｎｉｚｉｎｇ　ａｕｔｈｏｒｉｔｙ）または階層を含むのではなく、むしろパズルチェッカが消印状態を保持する調整ノードの集まりにその照会を分散させることができるようにすることが好ましい。一構成において、ピアノードの集まりは、消印データベースがピアツーピアネットワークに分散される分散された検索サービスを実施する。こうしたノードのネットワークは、キーの大きい集まりについてのキーから値へのマッピング機能を実装する。この場合、パズル識別子がキーとして使用される。所与のキーについてマッピングが存在する場合、対応するパズルには消印が施されている。こうしたＰ２Ｐネットワークを実行可能にする好適な機構が（非特許文献６）に記載されており、そのどんな部分も排除することなく、示唆するすべてについてその全体を参照により本明細書に組み込む。

【００４３】

複数の消印サーバを使用することはいくつかの利点を有する。つまり、各個々のパズルチェッカは消印サーバの同じ集まりに依存する必要がない、受信者によって信頼される消印サーバは送信者によって信頼される必要がない、消印サーバ間の十分な冗長をもってピアツーピアネットワークを形成する相互に疑わしい隣接するサーバによって消印システムをホストすることができるという利点がある。

【００４４】

本発明の一実施形態によれば、複数のパズルおよび解答は、複数の受信者向けのメッセージに含まれる。好ましい実施形態は、それが送信する各メッセージの各コピーが適切な数のパズル－解答を確実に有するようにするＳＭＴＰサーバなどのメール転送エージェントを備える。ＳＭＴＰ転送機能は容易に変更され、一般にそれらが転送するメッセージのヘッダーを操作する必要があるため、一意のパズル－解答が確実に異なるメール転送エージェント向けのメッセージとバンドルされるようにすることができる。例えば、メッセージが異なる５つのメールサーバの１０人の受信者に向けられており、１０個の一意のパズル－解答を有している場合、ＳＭＴＰサーバは、２つの一意のパズル－解答を確実に５つの各メールサーバ向けのメッセージコピーとバンドルするようにする。同様に、ターゲットのメールサーバが宛先メッセージを配信すると、（受信者のメールアプリケーションでパズルチェックが行われる実施形態において）各受信者は、単一の一意のパズル－解答を受信するだけである。各受信者は、メッセージの他の受信者によって受信される任意のパズル－解答を受信しないことが好ましい。これは、ある受信者が、消印サーバによってパズルの一意の識別子を消印することによって、別の受信者向けのメッセージのコピーを早まって無効にするのを防ぐ。さらに、メール転送エージェントレベルでパズル－解答の配布を行うことによって、受信者は、複数のパズル－解答のどれがその受信者に向けられたものであるかを決定する必要がない。この問題は、ブラインドカーボンコピー機能を使用して一部の受信者が「隠されている」場合さらに悪化する。

【００４５】

単一のＥメールメッセージの個々の受信者に一意のパズル－解答を保証する上記の戦略は、本発明の一実施形態において、同様に配布先リストのマネージャによって使用される。メッセージ送信者は、十分な数のパズル－解答を作成し、それらを配布されるメッセージとともに配布先リストマネージャに渡す。次いで配布先リストマネージャは、配布先リスト加入者に転送するメッセージの複数のコピーにパズル－解答を分ける。このように、送信者は、送信者には知られていない可能性はあるが、配布先リストの加入者であり、したがってその送信者のメッセージを受信すべき受信者のパズル－解答を作成する。

【００４６】

図５は、本発明の一実施形態による、複数の受信者に複数のパズル－解答とともにメッセージを送信する一例を示している。送信者は、そのメールアプリケーション５０２を使用して６人の受信者向けのメッセージを作成し、パズル生成－解答器５０４は、６つの暗号パズルおよび解答Ｐ／Ｓ１～６　５０６を生成する。メッセージおよびパズル－解答５０６は送信者のメールサーバ５０８に送信され、メールサーバは、メッセージヘッダーを検査し、４つの異なるメールサーバが６人の受信者にサービスを提供することに気づく。送信者のメールサーバ５０８は、メッセージおよびパズル－解答のうちの２つＰ／Ｓ１～２を第１のメールサーバ５１０に送信し、Ｐ／Ｓ３を第２のメールサーバ５１２に、Ｐ／Ｓ４を第３のメールサーバ５１４に、２つのＰ／Ｓ５～６を第４のメールサーバ５１６に送信する。第１のメールサーバ５１０は、メッセージヘッダーを検査し、メッセージおよびパズル－解答のうちの一方Ｐ／Ｓ１を第１の受信者のメールアプリケーション５１８に、メッセージおよびパズル－解答のうちの第２のものＰ／Ｓ２を第２の受信者のメールアプリケーション５２０に配信する。第２のメールサーバ５１２は、メッセージおよびパズル－解答Ｐ／Ｓ３を第３の受信者のメールアプリケーション５２２に配信し、第３のメールサーバ５１４は、メッセージおよびパズル－解答Ｐ／Ｓ４を第４の受信者のメールアプリケーション５２４に配信する。これらの受信者の各メールアプリケーションは、その各々のパズル－解答が１つまたは２つの消印サーバ５２６および５２８で消印されていないことを確認するパズルチェッカとともに動作する。第４のメールサーバ５１６は、２つの消印サーバ５２６および５２８と通信するパズルチェッカ５３０とともに動作する。パズルチェッカ５３０がＰ／Ｓ５は消印されていないことを確認すると、第４のメールサーバ５１６は、メッセージを第５の受信者のメールアプリケーション５３２に配信する。パズルチェッカ５３０がＰ／Ｓ６は消印されていないことを確認すると、第４のメールサーバ５１６は、メッセージを第６の受信者のメールアプリケーション５３４に配信する。

【００４７】

次に図６を参照して、本発明の一実施形態によるパズルチェックの方法について説明する。この方法はパズルチェッカによって実行されること、およびパズルチェッカは、受信者のメールアプリケーションまたはメールサーバに配置されることが好ましい。パズルチェッカは、ステップ６０２で、メッセージ（または他のデジタルオブジェクト）を暗号パズル、解答、一意のパズル識別子、およびタイムスタンプとともに受信する。パズルチェッカは、ステップ６０４で、例えばある範囲閾値に対して、タイムスタンプを現在の時刻と比較することによってタイムスタンプが有効であることをチェックする。タイムスタンプが範囲閾値外にある（例えば古すぎる、またはクロック信号の伝播時間のずれ（ｃｌｏｃｋ　ｓｋｅｗ）によるものという説明では考えられないほど未来にある）場合、パズルチェッカは、ステップ６０６でメッセージを拒否する。そうでない場合、ステップ６０８で、パズルチェッカは、解答がパズルを解き、パズルが識別子およびタイムスタンプに対応していることを確認する。この方法で使用する暗号パズルはこの好適な性質を有しているため、確認ステップ６０８では、演算の能力および時間は相対的にみてほとんど必要ない。解答がパズルを解かない場合、ステップ６０６で、パズルチェッカはメッセージを拒否する。そうでない場合、ステップ６１０で、パズルチェッカは、一意の識別子およびタイムスタンプを消印サービスに送信する。さらにパズルチェッカは、ステップ６１０で、トランザクション識別子を送信する。この識別子は、乱数または疑似乱数生成器によって生成され、１２８ビットの長さより大きい数であることが望ましい。パズルチェッカは、

ユーザまたはパズルチェッカの設定した所定の時間内に消印サーバから応答を受信しない場合、ステップ６１０で、トランザクション識別子、一意の識別子、およびタイムスタンプを再送信する。パズルチェッカは、ステップ６１２で、消印サービスから応答を受信し、ステップ６１４で応答を検査する。消印サーバがパズル識別子を拒否した場合、ステップ６０６で、パズルチェッカはメッセージを拒否する。消印サーバがパズルを拒否しない場合、パズルチェッカは、ステップ６１６で、追加の消印サービスに問い合わせるかどうかを決定する。問い合わせる場合、パズルチェッカは、ステップ６１０に戻って、パズルの一意の識別子およびタイムスタンプを追加の消印サービスに送信し、その後のステップを繰り返す。そうでない場合、パズルチェッカは、ステップ６１８でメッセージを受諾する。

【００４８】

ステップ６０６に関して、一部の実施形態は、消印サーバによって識別子が拒否されたメッセージに対して様々な対応を行う。例えば、本発明の一実施形態において実行される１つの動作は、拒否されたメッセージを破棄し、システムから削除する。代替の動作は、拒否されたメッセージを優先度の低いビンに入れ、受信者が望んだ場合、受信者がその後メッセージを見ることができるようにする、またはスパムフィルタをメッセージに適用できるようにする。メール転送エージェントにあるパズルチェッカでは、メッセージを拒否する動作の１つは、メッセージを削除し、目的の受信者に配信しないことである。またはこれに替えて、パズルチェッカは、メッセージを削除するのではなく、拒否された識別子を有するものとしてマーク付けする。ＭＴＡは、指定済みの新しいヘッダーフィールドをメッセージに追加することによってメッセージにマーク付けして、メッセージ識別子が消印サーバによって拒否されたことを示すようにすることが好ましい。また、ＭＴＡは、メッセージに事前に存在する可能性のあるこうした指定済みの任意のヘッダーフィールドを削除する。指定済みのヘッダーフィールドを読み取ることによって、下流のＭＴＡまたはメールアプリケーションは、メッセージをスパムについてフィルタし、メッセージの優先度設定を変更し、または消印サーバの拒否に基づいて他の対応を行うことができる。拒否された識別子付きのメッセージの処理に使用される方法は、ユーザ、ＭＴＡ、またはＩＳＰの選択に従って構成されることが好ましい。

【００４９】

次に図７を参照して、本発明の一実施形態によるパズルを消印する方法について説明する。この方法は、消印サーバがパズルチェッカと通信して行うことが好ましい。消印サーバは、ステップ７０２で、暗号パズルの一意の識別子、タイムスタンプ、およびトランザクション識別子を受信する。ステップ７０３で、消印サーバは、トランザクション識別子がすでにそのデータベース内に存在しているかどうかをチェックする。存在している場合、消印要求は、例えば通信障害のためにその最初の要求に対する応答を受信しなかったパズルチェッカからの重複する要求となる。消印サーバは、ステップ７０４でパズルを受諾し、呼び出し側のパズルチェッカに受諾の通知を送信する。そうでない場合、このトランザクションは新しいものであり、消印サーバは、ステップ７０５で、一意の識別子をハッシュし、それをハッシュテーブルで探す。消印サーバは、ステップ７０６で、一意の識別子がハッシュテーブルに存在しているかどうかを決定する。一意の識別子がすでにハッシュテーブルに存在している場合、そのパズルを再利用するため、消印サーバは、ステップ７１８でパズルを拒否して、呼び出し側パズルチェッカに拒否の通知を送信するようにする。そうでない場合、消印サーバは、ステップ７０９で、関連のハッシュテーブルをチェックするかどうかを決定する。関連のハッシュテーブルは、例えばこの消印サーバと通信するリモート消印サーバに配置されている。関連のハッシュテーブルがチェックされない場合、タイムスタンプおよび一意の識別子のハッシュは、ステップ７１０で、消印サーバのハッシュテーブルに格納され、消印サーバは、ステップ７０４でパズルを受諾し、呼び出し側パズルチェッカに受諾の通知を送信する。さらに、ステップ７１０で、受諾の通知が失敗した場合、パズルチェッカが消印サーバに対して再度照会を行うことができるようにするため、トランザクション識別子が格納される。トランザクション識別子は、パズル

識別子の寿命よりかなり短い、限られた時間だけ格納されるのが望ましい。そうでない場合、ステップ７１４で、一意の識別子が関連のハッシュテーブル内で探される。ステップ７１６で、消印サーバは、一意の識別子が関連のハッシュテーブルに入れられているかどうかを決定する。関連のハッシュテーブルに入れられている場合、消印サーバは、ステップ７０８でパズルを拒否する。そうでない場合、サーバは、ステップ７０９に戻って、別の関連のハッシュテーブルがチェックされるかどうかを決定する。

【００５０】

ハッシュテーブルは、図７の方法で使用され、データを有効に格納することができるようにすることが好ましいものの、データベース機能に役立つ任意のデータ構造を使用することができる。さらに、ハッシュテーブルは、タイムスタンプが例えば１５日など所与の閾値を超えたエントリを削除することによって、定期的にクリーンアップされることが好ましい。これによって、ハッシュテーブルのサイズが低減するので消印サーバのパフォーマンスが向上する。さらに、かなり古いエントリを削除することは、一般にユーザに影響を与えない。というのは、図６に関する方法で説明したように、パズルチェッカは、おそらく消印サーバを呼び出す前に古いメッセージを拒否するからである。

【００５１】

また、パズル識別子の一意性と消印サーバによって要求されるデータ構造のサイズとの間にはトレードオフもある。より小さい識別子はあまり記憶域を必要としないが、一意ではない可能性がより高いという危険性があり、それによってパズルチェッカによる「偽陽性」がもたらされることになる。偽陽性のコストは、パズルチェックシステムの特定の実装に左右される（例えば一部のパズルチェッカは、一意ではない識別子付きのメッセージを削除するが、別のパズルチェッカは、そのメッセージを削除せず、優先度の低いビンに入れる）。この偽陽性のためのコストは、消印サーバによって実装されたパズルの満了時間に加えて、一意の識別子の長さを選択する際の検討要因となる。１２８ビットの識別子は、図２に関連して上述したように、偽陽性のリスクは低いが、より小さい識別子も実際には可能である。

【００５２】

本発明の実施形態は、Ｅメールメッセージの配信に限定されない。本発明の実施形態は、情報がデジタルで配信される分散されたシステムの用途での情報のやり取りの速度を制御するため、一般に適用可能である。

【００５３】

本発明の実施形態は、暗号パズルの使用に限定されない。代替として、例えばＨｕｍａｎ Ｉｎｔｅｒａｃｔｉｖｅ Ｐｒｏｏｆ（ＨＩＰ）パズルなどの非暗号パズルが使用される。ＨＩＰ例は、コンピュータモニタ上に表示される歪んだ１組の文字を含み、ユーザは、文字を識別することが求められる。本発明の一実施形態において、サードパーティは、こうしたパズルを生成し、別のパーティが人間の解答をチェックするようにそれらをエンコードする。ＨＩＰパズルの例は、非特許文献７に開示されており、そのどんな部分も排除することなく、示唆するすべてについてその全体を参照により本明細書に組み込む。

【００５４】

本発明の原理を適用できる多くの可能な実施形態を考慮して、図面との関連で本明細書に記載した実施形態は、例示的なものにすぎず、本発明の範囲を限定するものとみなされるべきではないことを理解されたい。例えば、実施形態の例は、本発明の意図から逸脱することなく構成および詳細について変更できることを当業者は理解されよう。本発明は、ソフトウェアモジュールまたは構成要素の観点で説明しているが、これらは、ハードウェア構成要素に等しく置き換えることができることを本技術分野の技術者は理解されよう。したがって、本明細書に記載した本発明は、特許請求の範囲、およびその等価物の範囲内に含まれ得るすべての実施形態を含む。

【図面の簡単な説明】

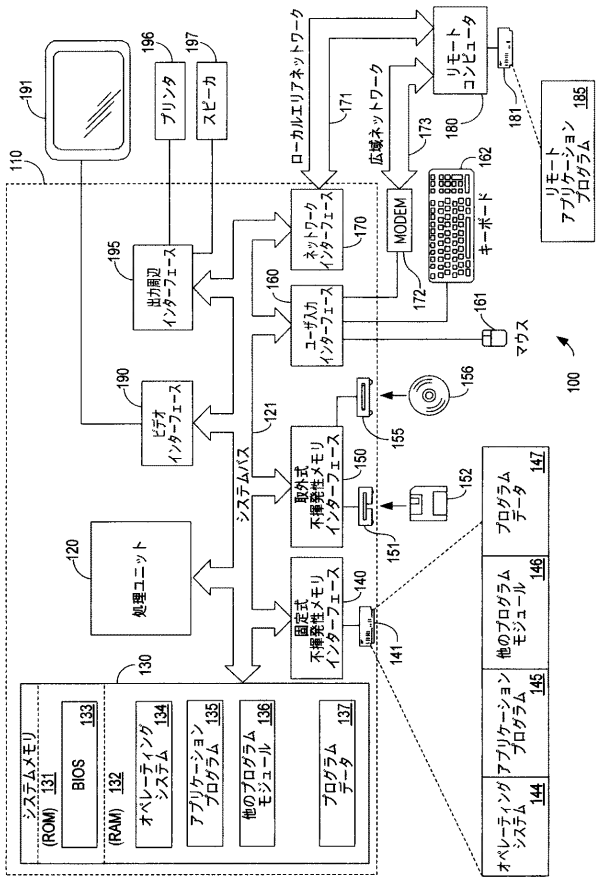
【００５５】

【図１】本発明の一実施形態による暗号パズルの消印サービスを実行するコンピューティ

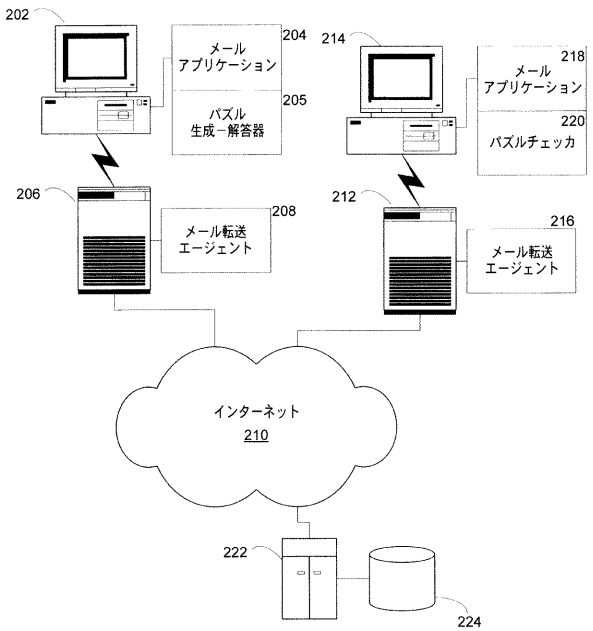
ング装置のアーキテクチャ例を示す概略図である。
【図２】本発明の一実施形態による消印サービスを含むネットワーク通信構成例を示す図である。
【図３ａ】本発明の一実施形態による暗号パズルの消印に使用する構成要素アーキテクチャ例を示す図である。
【図３ｂ】本発明の一実施形態による暗号パズルの消印に使用する構成要素アーキテクチャ例を示す図である。
【図４】本発明の一実施形態による複数の消印サーバの分散システムを示す図である。
【図５】本発明の一実施形態による複数の暗号パズルおよび複数の消印サーバを使用して複数の受信者向けに単一のメッセージを送信する例を示すネットワーク図である。
【図６】本発明の一実施形態による暗号パズルをチェックする方法を示すフロー図である。
【図７】本発明の一実施形態による消印サーバを作動させる方法を示すフロー図である。
【符号の説明】
【００５６】
１００　コンピューティングシステム環境
１１０　コンピュータ
１２０　処理ユニット
１２１　システムバス
１３０　システムメモリ
１３４　オペレーティングシステム
１３５　アプリケーションプログラム
１３６　他のプログラムモジュール
１３７　プログラムデータ
１４０　固定式不揮発性メモリインターフェース
１４４　オペレーティングシステム
１４５　アプリケーションプログラム
１４６　他のプログラムモジュール
１４７　プログラムデータ
１５０　取外式不揮発性メモリインターフェース
１６０　ユーザ入力インターフェース
１６１　マウス
１６２　キーボード
１７０　ネットワークインターフェース
１７１　ローカルエリアネットワーク
１７３　広域ネットワーク
１８０　リモートコンピュータ
１８５　リモートアプリケーションプログラム
１９０　ビデオインターフェース
１９５　出力周辺インターフェース
１９６　プリンタ
１９７　スピーカ
２０４　メールアプリケーション
２０５　パズル生成－解答器
２０８　メール転送エージェント
２１０　インターネット
２１８　メールアプリケーション
２２０　パズルチェッカ
２１６　メール転送エージェント
３０２　メールアプリケーション

３０４　パズル生成－解答器
３１０　メールアプリケーション
３１２　パズルチェッカ
３１４　消印サーバ
３１６　データベース
３５０　パズル生成－解答器
３５４　メールアプリケーション
３５８　パズルチェッカ
３６０　消印サーバ
３６２　データベース
３６４　メールアプリケーション
４０２　調整消印サーバ
４０６　パズルチェッカ
５０２　メールアプリケーション
５０４　パズル生成－解答器
５０６　パズル／解答１～６
５１８　メールアプリケーション
５２０　メールアプリケーション
５２２　メールアプリケーション
５２４　メールアプリケーション
５２６　消印サーバ
５２８　消印サーバ
５３０　パズルチェッカ
５３２　メールアプリケーション
５３４　メールアプリケーション

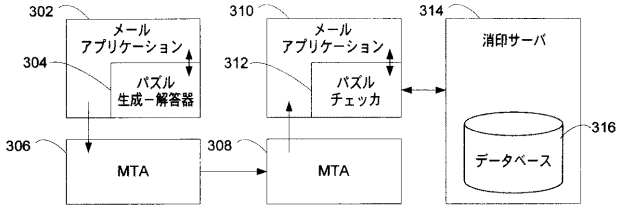
【図１】



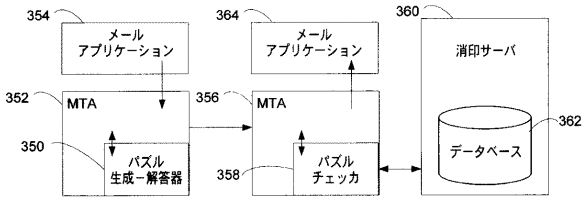
【図２】



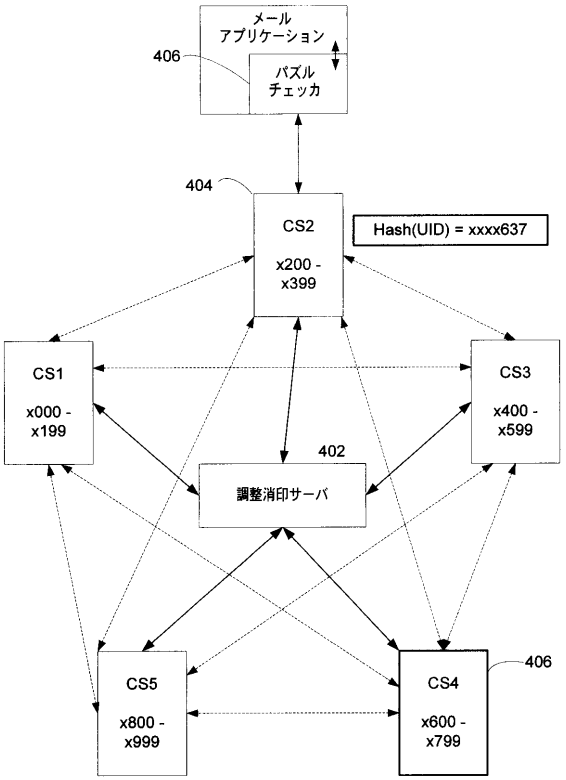
【図３ａ】



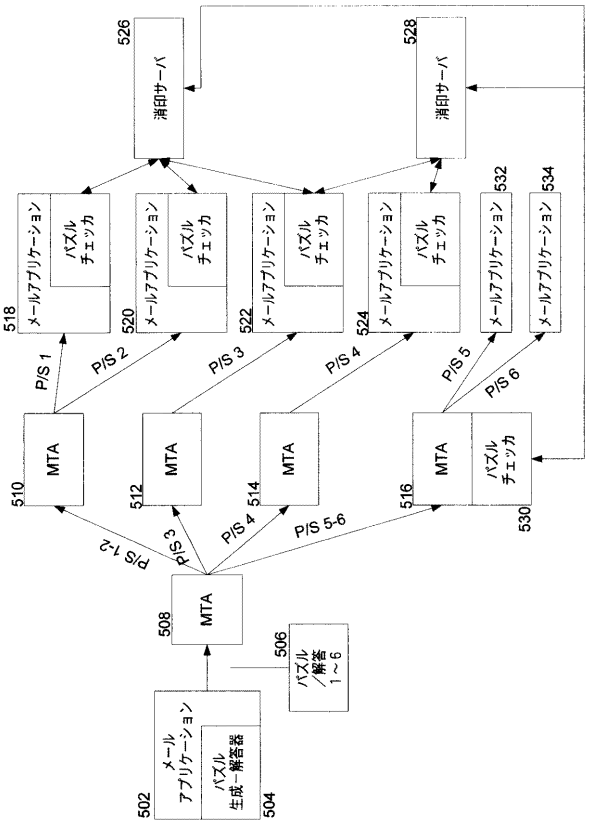
【図３ｂ】



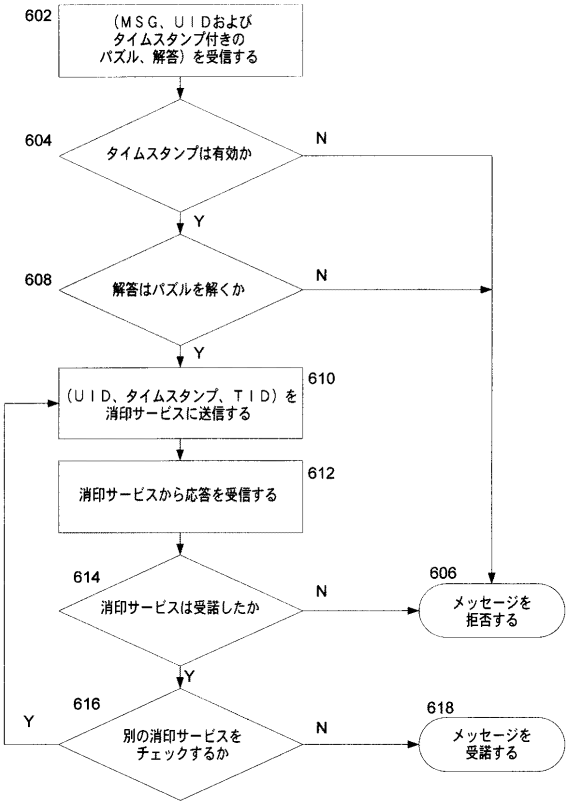
【図４】



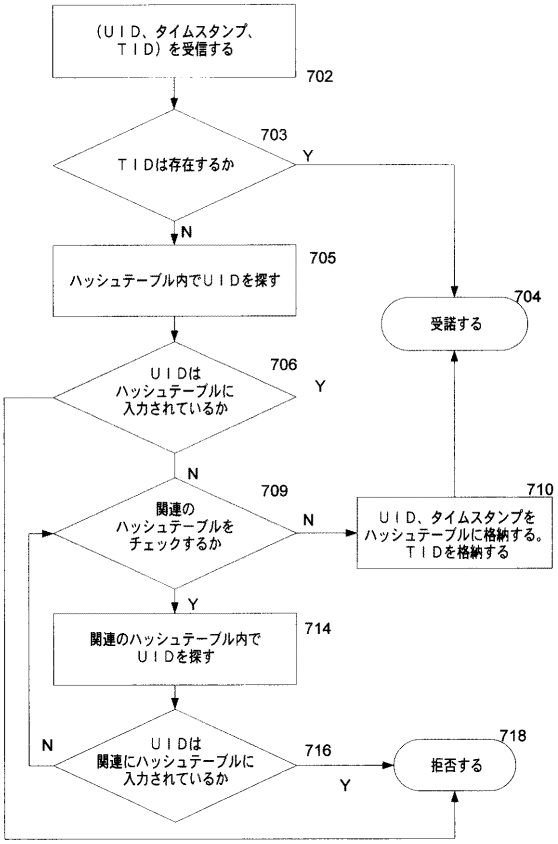
【図５】



【図６】



【図７】


（ＵＩＤ、タイムスタンプ、
ＴＩＤ）を受信する
702
703
ＴＩＤは存在するか
Y
N
705
ハッシュテーブル内でＵＩＤを探す
704
受諾する
706
ＵＩＤは
ハッシュテーブルに
入力されているか
Y
N
709
関連の
ハッシュテーブルを
チェックするか
N
710
ＵＩＤ、タイムスタンプを
ハッシュテーブルに格納する。
ＴＩＤを格納する
Y
714
関連のハッシュテーブル内で
ＵＩＤを探す
N
ＵＩＤは
関連にハッシュテーブルに
入力されているか
716
718
拒否する
Y

フロントページの続き

(72)発明者　エドワード　ピアース　ウッバー
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内
(72)発明者　マイケル　バロウズ
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

Ｆターム(参考) 5K030 GA04　GA15　HA06　KA07　LC15　LD17

【外国語明細書】
2005285116000001.pdf