(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2008-193667
(P2008-193667A)
(43)公開日　平成20年8月21日(2008.8.21)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32 (2006.01)		H04L	9/00	675A	5J104

審査請求 未請求　請求項の数 11　ＯＬ　（全 21 頁）

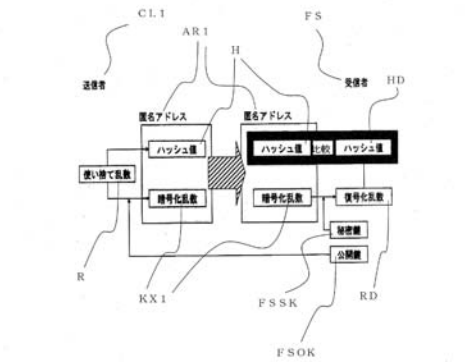
(21)出願番号　特願2008-211 (P2008-211)
(22)出願日　平成20年1月4日 (2008.1.4)
(31)優先権主張番号　特願2007-5235 (P2007-5235)
(32)優先日　平成19年1月12日 (2007.1.12)
(33)優先権主張国　日本国 (JP)

(71)出願人　304023994
国立大学法人山梨大学
山梨県甲府市武田四丁目４番３７号
(74)代理人　100119297
弁理士　田中　正男
(72)発明者　山崎　晴明
山梨県甲府市武田４丁目３番１１号　国立大学法人山梨大学内
(72)発明者　美濃　英俊
山梨県甲府市武田４丁目３番１１号　国立大学法人山梨大学内
(72)発明者　渡辺　喜道
山梨県甲府市武田４丁目３番１１号　国立大学法人山梨大学内

Ｆターム(参考)　5J104 AA08 LA01 LA05 NA12 PA08 PA17

(54)【発明の名称】秘匿通信方法

(57)【要約】
【課題】
秘匿通信方法として用いられるオニオンルーティングが有する、通信ルート内のコンピュータにシステムダウンがあるとその先へ一切継続されなくなるという問題や、多重化暗号化を使用することでシステムやトラフィックが重くなるといった問題を解決することを課題とする。
【解決手段】
情報提供元のクライアントは、自らが接続している情報サーバ、送りたい先の機能サーバ、機能サーバが接続している情報サーバ、のそれぞれの公開鍵を使用して、乱数の暗号化とそのハッシュ値算出を行い、各々のサーバは自らの秘密鍵を使って解読してハッシュ値との比較を行うことで、自分に関係するルートであるか否かを判断する通信方法であり、これにより、情報提供元や情報提供先を秘匿したまま情報提供できるだけでなく、情報提供先である機能サーバから提供内容に対する応答も匿名を維持したまま可能とする。
【選択図】　図３



【特許請求の範囲】
【請求項１】
あらかじめ定めたルールによりメッセージを回送させるループネットワークに接続し、自分の公開鍵を公開している複数の通信サーバと、前記通信サーバの配下として接続し、自分の公開鍵を公開している機能サーバとクライアントとを含んでなる通信ネットワークにおける秘匿通信方法において、前記クライアントは、ランダムビット列Ｒを生成し、該Ｒを送信先の前記機能サーバの公開鍵により暗号化した符号列ＫＸ１と、前記Ｒのハッシュ値Ｈを生成し、前記ＫＸ１と前記Ｈを送信先の秘匿アドレス１（ＫＸ１，Ｈ）とし、前記機能サーバが接続する前記通信サーバの公開鍵により、前記Ｒを暗号化した符号列ＴＸ１を生成し、前記ＴＸ１と前記Ｈを送信先の通信サーバの秘匿アドレス２（ＴＸ１，Ｈ）を生成し、前記秘匿アドレス１（ＫＸ１，Ｈ）と前記秘匿アドレス２（ＴＸ１，Ｈ）とを含むメッセージを自分が接続する前記通信サーバに送信し、前記通信サーバは回送されてくる前記メッセージのＴＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを比較し、一致した場合は、配下のクライアントと機能サーバとに前記メッセージを送信し、もしくは、該通信サーバで保持した後、前記配下のクライアントもしくは前記機能サーバからの要求時に前記メッセージを送信し、前記クライアントと前記機能サーバは、前記ＫＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は自分宛のメッセージであるとして受信することを特徴とする秘匿通信方法。
【請求項２】
前記クライアントは、前記メッセージを送信する際に前記Ｒを自分の公開鍵で暗号化した符号列ＣＸ１生成し、前記ＣＸ１と前記Ｈとからなる秘匿アドレス３（ＣＸ１，Ｈ）と、自分が接続する通信サーバの公開鍵で前記Ｒを暗号化し、符号列ＴＸ２を生成し、前記ＴＸ２とＨとからなる秘匿アドレス４（ＴＸ２、Ｈ）を生成し、前記秘匿アドレス３（ＣＸ１，Ｈ）と前記秘匿アドレス４（ＴＸ２、Ｈ）とを前記メッセージに含めて送信することを特徴とする請求項１に記載の秘匿通信方法。
【請求項３】
前記機能サーバは、前記秘匿アドレス３（ＣＸ１，Ｈ）及び前記秘匿アドレス４（ＴＸ２、Ｈ）とを含めて、自宛に送信されてきたメッセージのレスポンスを自分の接続する通信サーバに返信することを特徴とする請求項１又は２に記載の秘匿通信方法。
【請求項４】
前記通信サーバは、前記ＴＸ２を自分の秘密鍵で復号化し、そのハッシュ値と前記Hとを照合し、一致した場合は配下のクライアント及び／又は機能サーバに送信することを特徴とする請求項１から３のいずれかに記載の秘匿通信方法。
【請求項５】
前記クライアントは、前記ＣＸ１を自分の秘密鍵で復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は自宛のレスポンスであるとし、受信することを特徴とする請求項１から４のいずれかに記載の秘匿通信方法。
【請求項６】
前記クライアントは、自分が接続する通信サーバにメッセージを送信する際に、メッセージの本文にパスワードを付け、該パスワードを送信先の機能サーバの公開鍵により暗号化し、暗号パスワードＰＸ１を生成し、前記メッセージに含めて送信することを特徴とする請求項１から５のいずれかに記載の秘匿通信方法。
【請求項７】
前記機能サーバは自宛のメッセージを受信した際に、前記ＰＸ１を自秘密鍵で復号化し、前記本文を解読することを特徴とする請求項６に記載の秘匿通信方法。
【請求項８】
前記機能サーバは前記レスポンスを返信する際に、前記暗号パスワードＰＸ１によりレスポンスの本文にパスワードをかけて返信することを特徴とする請求項６又は７に記載の秘匿通信方法。
【請求項９】

前記クライアントは、自宛のレスポンスを受信した際に、前記ＰＸ１により前記レスポンスの本文を解読することを特徴とする請求項８に記載の秘匿通信方法。
【請求項１０】
前記クライアント、及び前記機能サーバは、自分が接続する通信サーバに対し、定期的なメッセージの取得を実行することを特徴とする請求項１か９のいずれかに記載の秘匿通信方法。
【請求項１１】
あらかじめ定めたルールによりメッセージを回送させるループネットワークに接続し、自分の公開鍵を公開している複数の通信サーバと、前記通信サーバの配下として接続し、自分の公開鍵を公開している機能サーバとクライアントとを含んでなる通信ネットワークにおける秘匿通信方法において、前記クライアントは、ランダムビット列Ｒを生成し、該Ｒを送信先の機能サーバの公開鍵により暗号化した符号列ＫＸ１と、前記Ｒのハッシュ値Ｈを生成し、前記ＫＸ１と前記Ｈを送信先の秘匿アドレス１（ＫＸ１，Ｈ）とし、前記機能サーバが接続する通信サーバの公開鍵により、前記Ｒを暗号化した符号列ＴＸ１を生成し、前記ＴＸ１と前記Ｈを送信先の通信サーバの秘匿アドレス２を生成し、前記秘匿アドレス１（ＫＸ１，Ｈ）と前記秘匿アドレス２（ＴＸ１，Ｈ）とし、前記メッセージを送信する際に前記Ｒを自分の公開鍵で暗号化した符号列ＣＸ１生成し、前記ＣＸ１と前記Ｈとからなる秘匿アドレス３（ＣＸ１，Ｈ）と、自分が接続する通信サーバの公開鍵で前記Ｒを暗号化し、符号列ＴＸ２を生成し、前記ＴＸ２とＨとからなる秘匿アドレス４（ＴＸ２、Ｈ）を生成し、少なくとも前記秘匿アドレス１（ＫＸ１，Ｈ）と前記秘匿アドレス３（ＣＸ１，Ｈ）と前記秘匿アドレス４（ＴＸ２、Ｈ）とをを含むメッセージを携帯可能な記憶媒体へ記録し、前記通信サーバに接続されたデータ入力端末から該記憶媒体より入力された前記記憶媒体に記録したメッセージのＴＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを比較し、一致した場合は、配下のクライアントと機能サーバとに前記メッセージを送信し、前記クライアントと前記機能サーバは、前記ＫＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は自分宛のメッセージであるとして受信することを特徴とする秘匿通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報を提供する提供元を秘匿したまま提供先に内容を秘密裏に受け渡す技術であって、さらには受け取った提供先が提供元を知らないままで、応答を提供元に返すことを可能とする秘匿通信方法に関する。
【背景技術】
【０００２】
情報提供者が匿名性を保ったまま情報提供先である例えば調査会社にコンピュータシステムを利用して情報を提供する匿名情報提供方法（情報提供元を秘匿した通信方法）としては、従来、情報提供者の本人確認を行うための第三者として信頼性確認者を設定するとともに、また保存情報の公開サービスを行うＢＢＳ（保存情報公開サービス）を設定し、情報提供者から信頼性確認者に情報提供者の本人確認を依頼して本人確認を行った後、情報提供者が匿名通信路を介して調査会社に情報を送信し、調査会社では情報提供者からの情報を受信した後において、情報提供者を特定する必要がある場合、信頼性確認者に情報提供者の身元確認のための問い合わせを行い、これにより情報提供者を特定することができるものが一般的に用いられてきている。
【０００３】
しかしながらこの方法では、信頼できる第３者を構築することに困難があるため、実際の運用上では大きな問題となっている。
インタネットの普及に伴い、悪意あるユーザの盗聴、改ざん等から通信内容を保全する様々な提案や製品開発がなされている。
【０００４】

一方、通信内容のみならず、宛先や発信元を秘匿することの必要性もしばしば指摘されるところである。宛先や発信元のアドレスはヘッダ情報を盗聴したり、経由したルータの情報をトレースしたりすることで突き止めることができる。
したがってＩＰアドレス等のヘッダ情報を秘匿する必要性が生ずるが、暗号化等の秘匿手法をヘッダに直接的に適用すると、ルータ等の通信機器を経由することができなくなってしまう。このような問題点を解決すべく、様々な手法が最近提案されるようになってきている。
そこで編み出された代表的な方法として、オニオンルーティングを用いた匿名通信方法が提案されている。（特許文献１）

【０００５】

以下簡単にこの方法を説明する。
図１はオニオンルーティングを用いた匿名通信方法を説明するフローチャートである。
各ステップのＳ０からＳ５で用いられているＡｄｒ１からＡｄｒＮ－１は情報提供者と情報提供先とをつなぐ経路での通信装置（以下サーバとする）のアドレス(宛先)である。そして情報提供元がＡｄｒ０であり、情報提供先がＡｄｒＮである。

【０００６】

この図において（）でくくられている内容が暗号化されており、その（）の暗号化を解くことができる鍵を各サーバが有している。この鍵をＫｙＪとした。尚、ＩとＪはこのフローチャートを説明するためのカウンターであり、実際の通信に必要なものではない。
ステップＳ０において、Ａｄｒ０のアドレス（宛先）は情報提供元のものである。情報提供元から最初に送るアドレスＡｄｒ１のサーバに対して、オニオンルーティング情報である（Ａｄｒ２（Ａｄｒ３（・・・（ＡｄｒＮ）・・））を情報提供先へ提供したい提供情報と一緒に送信する。

【０００７】

ステップＳ１の最初であるＩ＝Ｎ－１、Ｊ＝１の状態では、宛先がアドレスＡｄｒ１のサーバであって、Ａｄｒ１サーバでは解除キーＫｙ１を有しており、このＫｙ１を用いて（）を解除してＡｄｒ２が次ぎの宛先であること取得する。
そしてステップＳ２で次のＡｄｒ２サーバに対して次のオニオンルーティング情報である（Ａｄｒ３（Ａｄｒ４・・・（ＡｄｒＮ）・・））を受け取った提供情報とともに送る。
ステップＳ３とステップＳ４はこのフローチャートの説明のために設置したカウンター加減算をその判定である。

【０００８】

このように、以下順次Ａｄｒ３、Ａｄｒ４へと送られてアドレスＡｄｒＮの装置へ提供情報が伝達される。
このときＡｄｒ１からＡｄｒＮはそれぞれ解除キーＫｙ１からＫｙＮで暗号化が解けるように暗号化されているものである。
このような情報伝達を行うことにより、途中のサーバではその前後のサーバのアドレスしかわからないため、情報提供元のＡｄｒ０を特定するためには、すべてのサーバから情報を取得しなければならない為、その結果として情報提供元は秘匿される。

【特許文献１】特開２００４－２２９０７１

【発明の開示】

【発明が解決しようとする課題】

【０００９】

この方法では順次解読により宛先を特定して行き何回目かに目的とする宛先に届くよう宛先が多重暗号化されているため、その繰り返しで経由するコンピュータのどれかひとつでもダウンしていると進まなくなる。また頻繁に往復する情報授受をネットワークで適用する場合では、各ノードの処理に負荷がかかることからネットワークが重たくなってトラフィック障害を生じる恐れが付きまとう。原則として情報提供元で使用する装置またはそれを接続しているサーバにおいて、経由する全てのサーバの鍵に対応した暗号化を知っておく必要があるため、情報の漏えいの面でも危険がある。

【００１０】
本発明の方式はこのような課題を解決するもので、送信元のアドレス秘匿を受信者に対しても行うことができることを目的とする。さらに送信元を秘匿したうえで、受信者から応答の受信を可能にすることを目的とする。
【課題を解決するための手段】
【００１１】
請求項１に記載の発明は、あらかじめ定めたルールによりメッセージを回送させるループネットワークに接続し、自分の公開鍵を公開している複数の通信サーバと、前記通信サーバの配下として接続し、自分の公開鍵を公開している機能サーバとクライアントとを含んでなる通信ネットワークにおける秘匿通信方法において、前記クライアントは、ランダムビット列Ｒを生成し、該Ｒを送信先の前記機能サーバの公開鍵により暗号化した符号列ＫＸ１と、前記Ｒのハッシュ値Ｈを生成し、前記ＫＸ１と前記Ｈを送信先の秘匿アドレス１（ＫＸ１，Ｈ）とし、前記機能サーバが接続する前記通信サーバの公開鍵により、前記Ｒを暗号化した符号列ＴＸ１を生成し、前記ＴＸ１と前記Ｈを送信先の通信サーバの秘匿アドレス２（ＴＸ１，Ｈ）を生成し、前記秘匿アドレス１（ＫＸ１，Ｈ）と前記秘匿アドレス２（ＴＸ１，Ｈ）とを含むメッセージを自分が接続する前記通信サーバに送信し、前記通信サーバは回送されてくる前記メッセージのＴＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを比較し、一致した場合は、配下のクライアントと機能サーバとに前記メッセージを送信し、もしくは、該通信サーバで保持した後、前記配下のクライアントもしくは前記機能サーバからの要求時に前記メッセージを送信し、前記クライアントと前記機能サーバは、前記ＫＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は自分宛のメッセージであるとして受信することを特徴とする秘匿通信方法としたことにより、情報発信者が誰であって、情報提供先がどこであるかを秘匿したまま、情報提供を可能とした。
【００１２】
請求項２に記載の発明は、前記クライアントは、前記メッセージを送信する際に前記Ｒを自分の公開鍵で暗号化した符号列ＣＸ１生成し、前記ＣＸ１と前記Ｈとからなる秘匿アドレス３（ＣＸ１，Ｈ）と、自分が接続する通信サーバの公開鍵で前記Ｒを暗号化し、符号列ＴＸ２を生成し、前記ＴＸ２とＨとからなる秘匿アドレス４（ＴＸ２、Ｈ）を生成し、前記秘匿アドレス３と４とを前記メッセージに含めて送信することを特徴とする請求項１に記載の秘匿通信方法としたことにより、提供者を秘匿したまま応答を返すことが出来るようにした。
【００１３】
請求項３に記載の発明は、前記機能サーバは、前記秘匿アドレス３及び前記秘匿アドレス４とを含めて、自宛に送信されてきたメッセージのレスポンスを自分の接続する通信サーバに返信することを特徴とする請求項１又は２に記載の秘匿通信方法としたことにより、提供された匿名データに関して提供者を秘匿したまま質問などの応答メッセージを返すことが出来るようにした。
【００１４】
請求項４に記載の発明は、前記通信サーバは、前記ＴＸ２を自分の秘密鍵で復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は配下のクライアント及び／又は機能サーバに送信することを特徴とする請求項１から３のいずれかに記載の秘匿通信方法としたことにより、秘匿したままで通信サーバが取り込み可能とするかに関しての機密性を更に向上した。
【００１５】
請求項５に記載の発明は、前記クライアントは、前記ＣＸ１を自分の秘密鍵で復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は自宛のレスポンスであるとし、受信することを特徴とする請求項１から４のいずれかに記載の秘匿通信方法としたことにより、秘匿したままで機能サーバが取り込み可能とするかに関しての機密性を更に向上した。

【００１６】
請求項６に記載の発明は、前記クライアントは、自分が接続する通信サーバにメッセージを送信する際に、メッセージの本文にパスワードを付け、該パスワードを送信先の機能サーバの公開鍵により暗号化し、暗号パスワードＰＸ１を生成し、前記メッセージに含めて送信することを特徴とする請求項１から５のいずれかに記載の秘匿通信方法とした。
【００１７】
請求項７に記載の発明は、前記機能サーバは自宛のメッセージを受信した際に、前記ＰＸ１を自秘密鍵で復号化し、前記本文を解読することを特徴とする請求項６に記載の秘匿通信方法とした。これらにより、提供メッセージの解読セキュリティーを高くした。
【００１８】
請求項８に記載の発明は、前記機能サーバは前記レスポンスを返信する際に、前記暗号パスワードＰＸ１によりレスポンスの本文にパスワードをかけて返信することを特徴とする請求項６又は７に記載の秘匿通信方法とした。
【００１９】
請求項９に記載の発明は、前記クライアントは、自宛のレスポンスを受信した際に、前記ＰＸ１により前記レスポンスの本文を解読することを特徴とする請求項８に記載の秘匿通信方法とした。これらにより、応答メッセージの解読セキュリティーを高くした。
【００２０】
請求項１０に記載の発明は、前記クライアント、及び前記機能サーバは、自分が接続する通信サーバに対し、定期的なメッセージの取得を実行することを特徴とする請求項１か９のいずれかに記載の秘匿通信方法としたことにより、オンデマンド取得としてネットワーク負荷を下げた。
【００２１】
請求項１１に記載の発明は、あらかじめ定めたルールによりメッセージを回送させるループネットワークに接続し、自分の公開鍵を公開している複数の通信サーバと、前記通信サーバの配下として接続し、自分の公開鍵を公開している機能サーバとクライアントとを含んでなる通信ネットワークにおける秘匿通信方法において、前記クライアントは、ランダムビット列Ｒを生成し、該Ｒを送信先の機能サーバの公開鍵により暗号化した符号列ＫＸ１と、前記Ｒのハッシュ値Ｈを生成し、前記ＫＸ１と前記Ｈを送信先の秘匿アドレス１（ＫＸ１，Ｈ）とし、前記機能サーバが接続する通信サーバの公開鍵により、前記Ｒを暗号化した符号列ＴＸ１を生成し、前記ＴＸ１と前記Ｈを送信先の通信サーバの秘匿アドレス２を生成し、前記秘匿アドレス１（ＫＸ１，Ｈ）と前記秘匿アドレス２（ＴＸ１，Ｈ）とし、前記メッセージを送信する際に前記Ｒを自分の公開鍵で暗号化した符号列ＣＸ１生成し、前記ＣＸ１と前記Ｈとからなる秘匿アドレス３（ＣＸ１，Ｈ）と、自分が接続する通信サーバの公開鍵で前記Ｒを暗号化し、符号列ＴＸ２を生成し、前記ＴＸ２とＨとからなる秘匿アドレス４（ＴＸ２、Ｈ）を生成し、少なくとも前記秘匿アドレス１（ＫＸ１，Ｈ）と前記秘匿アドレス３（ＣＸ１，Ｈ）と前記秘匿アドレス４（ＴＸ２、Ｈ）とをを含むメッセージを携帯可能な記憶媒体へ記録し、前記通信サーバに接続されたデータ入力端末から該記憶媒体より入力された前記記憶媒体に記録したメッセージのＴＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを比較し、一致した場合は、配下のクライアントと機能サーバとに前記メッセージを送信し、前記クライアントと前記機能サーバは、前記ＫＸ１を自分の秘密鍵により復号化し、そのハッシュ値と前記Ｈとを照合し、一致した場合は自分宛のメッセージであるとして受信することを特徴とする秘匿通信方法としたことにより、全てのルートをオンラインにしなくても、情報提供者が自己を匿名としてデータを隔離された入力端末にて供給し、提供された匿名データを取得し、機能サーバが提供を受けられるようにした。
【発明の効果】
【００２２】
本発明によれば、情報提供者であるクライアントが特定されることなく、また、どの相談窓口や掲示板などの機能提供を行う機能サーバに提供したのかも秘匿されたまま、メッセ

ージ授受を行うことが出来る。さらに、誰から提供されたのかを知らないままに、提供された情報へ応答することも出来すべての授受が秘匿できる。

【発明を実施するための最良の形態】

【００２３】

次に図２、図３、図４を用いて、本発明のシステムと通信の手順とを概略説明する。なお、そのデータ（ここではメッセージＭＳと称する）の構成を含めた秘匿方法の説明、暗号化に関する詳細に関しては、この概略説明の後に行う。

【００２４】

（システム概要）

本提案手法はブロードキャスト通信（あるいはオンデマンド通信）と公開鍵暗号系を組み合わせたものであり、その特徴は、秘密鍵を（より正確には公開鍵によって暗号化されたチェックフィールドを）、一種のアドレスとして用いるという点である。

ブロードキャスト通信を効率的に行うために、アプリケーションレベルでのルーティングには、論理的なループをあらかじめ形成しておくというアプローチをとる。

なお、実装においてはブロードキャスト通信と論理的には等価であるが、帯域を節約するため、オンデマンドで無条件に情報を送付する方式を採用している。

【００２５】

（構成要素）

ネットワークの構成要素として次を考える。

（１）一般ユーザ：家庭、オフィスから匿名通信を利用するユーザであって図２ではクライアントＣＬ。説明のための送信者はクライアントＣＬ１

（２）通信サーバ：クライアントＣＬ（説明ではクライアントＣＬ１）からの匿名メッセージを受け付け、送信するサーバであって、図２では通信サーバＣＳ１、ＣＳ２、ＣＳ３、ＣＳ４、ＣＳ５（以下これらをＣＳと総称する）。また、クライアントＣＬ（機能サーバＦＳを含む）への匿名メッセージを受信、蓄積する。通信サーバ間に論理的なループ（ループネットワーク）を形成する。

【００２６】

（３）２次、３次通信サーバ：通信サーバＣＳ４の障害生起時に、代わりにサーバとなりうるノードである。たとえばＣＳ４がダウンした場合には、ＣＳ３がＣＳ４のクライアント全てを、自身のサブスクライバに追加して管理する。この多重化についてはごく一般的に方法により実現できるために、この説明は省略する。

（４）機能サーバ：一般ユーザにサービスを提供するサイトなどで、図２では通信サーバＣＳ４に接続している機能サーバＦＳ、例えば、相談窓口、健康相談カウンセラー、苦情受け付け窓口等である。

（５）サブスクライバ：図２において通信サーバＣＳ配下のクライアントＣＬ及び機能サーバＦＳ。なお、匿名性を保持するためには運用上、機能サーバＦＳと通信サーバＣＳ４とは物理的にも、組織体制的にも明確に分離されていなくてはならない。

【００２７】

（動作条件）

次に各構成要素に関して次の前提を置く。

【００２８】

（１）通信サーバＣＳ１、通信サーバＣＳ２、通信サーバＣＳ３、通信サーバＣＳ４、通信サーバＣＳ５の間でのメッセージの回る順序をあらかじめ決めておく。通信サーバがループ（リング）状に接続されたネットワークＬＮＷ（ループネットワーク、リングネットワーク）となる。

（２）通信サーバＣＳは自身のＩＰアドレスと公開鍵（たとえば通信サーバ４であれば公開鍵ＣＳ４ＯＫ）を、その直前の通信サーバＣＳ（前記の場合通信サーバ３）に通知しておく。

【００２９】

（３）機能サーバＦＳは自身の受け付けるメッセージＭＳの内容を、その機能サーバＦＳ

が属する通信サーバＣＳ４の公開鍵ＣＳ４ＯＫ及び自身の公開健ＦＳＯＫとともに宣言、公開する。例えば、専用の特定ウェブ上で、苦情受け付け、相談窓口等を宣言する。
（４）クライアントＣＬ及び機能サーバＦＳはいずれかの通信サーバにサブスクライバとして登録される。クライアントＣＬ１は以下の図２などで送信手順等で説明用に用いられる、メッセージを匿名で送りたいクライアントＣＬの一人である。
【００３０】
（送信手順）
今、クライアントＣＬ１から機能サーバＦＳに向かってデータを送信する場合を考える。そのときの手順は以下となる。
【００３１】
（１）クライアントＣＬ１は利用したい機能サーバＦＳが属する通信サーバＣＳ４の公開鍵ＣＳ４ＯＫ、機能サーバＦＳ自身の公開鍵ＦＳＯＫを入手する。
（２）クライアントＣＬ１は通信サーバＣＳ２に、公開鍵ＣＳ４ＯＫおよびＦＳＯＫで暗号化したメッセージＭＳを送信する。メッセージＭＳの構造は図４へ詳細を示した。
（３）通信サーバＣＳ２は、送信バッファにメッセージＭＳを蓄積する。
（４）通信サーバＣＳ２は、通信サーバＣＳ３に向かってメッセージＭＳを送信する。
【００３２】
（５）メッセージを受け取った通信サーバＣＳ３は、メッセージＭＳをコピーし、蓄積して、メッセージを通信サーバＣＳ４に送信する。以降、同様に各通信サーバは決められた順序にしたがってメッセージを転送、蓄積する。
（６）通信サーバＣＳ１からメッセージＭＳを受け取った通信サーバＣＳ２は自身の送信したメッセージＭＳがループネットワークＬＮＷを一巡したことを知りメッセージＭＳを消滅させる。
【００３３】
（７）各通信サーバＣＳは蓄積したメッセージＭＳを、それぞれの秘密鍵ＣＳＳＫで解読することを試みる。この場合、公開鍵ＣＳ４ＯＫで暗号化されたメッセージを解くことができるのは通信サーバＣＳ４のみであり、これを保存する。通信サーバＣＳ４以外の通信サーバＣＳは自分宛ではないことを知り、メッセージＭＳを保存バッファから削除する。
【００３４】
（受信手順）
これに対して、受信手順は以下となる。
（１）図２の例では通信サーバＣＳ４に機能サーバＦＳが接続されていることから、各クライアントＣＬと機能サーバＦＳは、接続している通信サーバＣＳ４からのブロードキャスト通信、もしくは、通信サーバＣＳ４に対するオンデマンドによる情報の受信によって、通信サーバＣＳ４に蓄積されたメッセージＭＳをすべて取り込み、メッセージＭＳの後に詳細な説明を行う特定フィールドＡＲ２に対し自身の秘密鍵ＣＳ４ＳＫで解読を試みる。もし解読できなければ、自分宛のメッセージＭＳではないと判断し、自バッファから取り除く。
【００３５】
（２）解読できた場合は、自分宛のメッセージＭＳであると解釈し、これを取り込む。例においては、機能サーバＦＳは、別の特定フィールドＡＲ１に対して自身の秘密鍵ＦＳＳＫで解読できる。
【００３６】
（３）一定期間経過するか、すべてのクライアントＣＬが取り込んでしまったメッセージＭＳは、通信サーバＣＳにより削除される。
なお、機能サーバＦＳが受け取ったメッセージ本文は秘匿するための暗号化も有効であって、送信本文（メッセージとしての本体）を秘匿するために、本文を機能サーバの公開鍵ＣＬ１ＯＫにより暗号化し、暗号パスワードＰＸ１を生成し、前記メッセージに含めて送信するのである。（図４）
【００３７】

（受信後の応答手順）
さらに、応答の送信手順は以下となる。
匿名メッセージに対する応答を必要とする場合は、図４にその構造を示したが、上述の送信手順（２）において、匿名メッセージの送信者であるクライアントＣＬ１は自らの公開鍵ＣＬ１ＯＫによって作成した匿名返信先である秘匿アドレスＡＲ３とそのハッシュ値（ＣＸ１，Ｈ）と、自分が接続する通信サーバの公開鍵で乱数ビット列Ｒを暗号化し、符号列ＴＸ２を生成し、このＴＸ２とハッシュ値とからなる秘匿アドレスＡＲ４（ＴＸ２、Ｈ）を暗号化メッセージＭＳの中へ含める。
【００３８】
機能サーバＦＳは応答を作成した上で送る際に、この受信したＡＲ３，ＡＲ４を宛先をして応信する。これによって匿名性を確保したまま、返信先を指定する。また返信内容を秘匿するために、受け取り時のＰＸ１と同様に使い拾てパスワード（具体的には乱数）を受信者の公開鍵ＣＬ１ＯＫで暗号化したものを同封する。
これらを前述に同様な手法で送信し、秘匿アドレスＡＲ３と秘匿アドレスＡＲ４を宛先として返信を送信する。図２によれば通信サーバＣＳ２を経由してクライアントＣＬ１へ戻したいので、秘匿アドレスＡＲ４が通信サーバ２で解かれて、その後秘匿アドレスＡＲ３を使ってクライアントＣＬ１へ届く。秘匿アドレスＡＲ３、秘匿アドレスＡＲ４の生成方法は、前述のとおりある。
【００３９】
（秘匿アドレス生成の説明）
以下に図３を使用して、送信元であるクライアントＣＬ１から機能サーバＦＳに対してあて先として用いる匿名アドレスＡＲ１の生成と確認の方法は以下の通りである。なお、機能サーバＦＳが接続している通信サーバＣＳ４に対する秘匿アドレスＡＲ２も同一の方法で生成されるので、詳細を省略する。
【００４０】
（１）匿名アドレスＡＲ１は以下のように作成する。
（１-１） 使い捨てのランダムビット列Ｒを用意する。
（１-２） ＭＤ５などの方法を用いて、ランダムビット列Ｒのハッシュ値Ｈを作成する。
（１-３） 一方で、ランダムピット列Ｒを受信者である機能サーバＦＳの公開健ＦＳＯＫで暗号化し、それをＫＸ１とする。
（１-４） ＫＸ１とＨを組にして、匿名アドレスＡＲ１=（ＫＸ１、Ｈ）とする。
【００４１】
(２）匿名アドレスＡＲ１は受信者を指定するが、受信者以外にはこのアドレスがどこを指しているかはわからない。
（３）受信者（この場合機能サーバＫＳ）は以下の手順で自分が受信者であることを知る。
（３-１） ＡＲ１中のＫＸ１を自分の秘密鍵で解読し解読乱数ＲＤを得る。
（３-２） その結果のハッシュ値ＨＤを求める。
（３-３） ＡＲ１中のＨとＨＤが等しければ自分宛とみなす。
【００４２】
以下にデータ構成の説明を図４により行う。
本アプリケーションプロトコルで利用されるメッセージフレームの形式を図４に示す。ＴＣＰプロトコルに対応するＴＣＰヘッダの他に、可変長フィールドに対応するためにすべてのフィールドにはフィールド長が宣言されている。図２の記号を用いて説明すると、各フィールドには、情報提供元クライアントＣＬ１から情報サーバＣＳ４へ渡すための秘匿アドレスＡＲ２について暗号化符号ＴＸ１を解読してハッシュ値Ｈと比較し、更に機能サーバＦＳへ渡すための秘匿アドレスＡＲ１があり暗号化符号ＫＸ１を解読してハッシュ値Ｈと比較し、また、機能サーバＦＳからクライアントＣＬ１に応答を戻すために、クライアントＣＬ１が接続されている情報サーバＣＳ２に渡すための秘匿アドレスＡＲ４の暗号

化符号ＴＸ２を解読してハッシュ値Ｈと比較し、さらにクライアントＣＬ１に渡すための秘匿アドレスＡＲ３の暗号化符号ＣＸ１を解読してハッシュ値Ｈと比較する。

【００４３】

その生成比較法（解読法）は前述の図３での説明の通りである。機能サーバＦＳではクライアントＣＬ１から来たことはわからないため、秘匿アドレスＡＲ３と秘匿アドレスＡＲ４の生成はクライアントＣＬ１自ら行い、初期の情報提供時のデータフィールドへ設定する（図４のとおり）。また、渡したいメッセージが付けられるが、機能サーバＦＳの公開鍵ＦＳＯＫで解読用のパスワードＰＸ１とともにメッセージＭＳを暗号化する。

【００４４】

（通信実験）

図５は、本発明の方式において、通信サーバより未読のすべてのメッセージをクライアント側に引き上げ、自分宛か否かを解読するために要する時間を測定した結果である。具体的には、通信サーバに１０００メッセージまでの未読メッセージを置き、クライアント側でこれを解読するのに要する時間を測定した。以下に実験環境と測定結果を示す。

【００４５】

（通信速度評価）

インターネットを介したメッセージ送信から受信までのターンアラウンドメッセージ数を１０００通まで増加させていった場合の、受信処理時間を図５に示す。

【００４６】

（実験環境）

（暗号化条件）

暗号化方式ＲＳＡ（鍵長は１０２４ビット）。ハッシュアルゴリズムＳＨＡ１。
メッセージ長暗号化前は１０３バイト、暗号化後は１１２パイト。
メッセージの暗号化方式ＡＥＳ（鍵長は２５６ビット）。

【００４７】

（ＰＣ等能力）

クライアントＰＣ・ＮＥＣ・ＶｅｒｓａＰｒｏ（登録商標）
　ＣＰＵ　ＰｅｎｔｉｕｍＭ７４０（登録商標）　１．７３ＧＨｚ
　メモリ　ＥＣＣ無しＤＤＲ２－ＳＤＲＡＭ　ＰＣ２－４２００　１２８０ＭＢ
　ＯＳ　ＷｉｎｄｏｗｓＰｒｏｆｅｓｓｉｏｎａｌ（ＳＰ２）（登録商標）
　ＮＩＣ　１０００ＢＡＳＥ－Ｔ／１００ＢＡＳＥ－Ｔｘ／１０ＢＡＳＥ
通信サーバ　Ｄｅ１１　Ｄｉｍｅｎｓｉｏｎ１１００（登録商標）
　ＣＰＵ　Ｉｎｔｅｌ（登録商標）Ｐｅｎｔｉｕｍ４（登録商標）
　メモリ　ＤＤＲＳＤＲＡＭ　ＰＣ３２００
　０Ｓ　ＵｂｕｎｔｕＬｉｎｕｘ７．０４（登録商標）
　ＮＩＣ　１００ＢＡＳＥ－Ｔｘ／１０ＢＡＳＥ－Ｔ
ネツトワーク（ＨＵＢ）１００ＢＡＳＥ－ＴＸ

【００４８】

（実験結果）

図５の中の破線Ｌ１は１０通９通までが自分宛のメッセージであった場合、実線Ｌ２は１０通中１通が自分宛のメッセージであった場合である。予想通り、メッセージ数の増加に伴い処理時間が線形に増加していく傾向が見られた。また１０００メッセージ中１００メッセージが自分宛てであった場合でも、（現実問題として生起するのはもっと少ないことが想定されるが）処理時間は約４秒で極り、十分実用に耐えうることが見込まれた。

【００４９】

（応用例１）

本発明の第１の応用は公開掲示板システムへの応用である。本応用例は、匿名通信システムの応用として、掲示板システムへ適用し本音で語ることが出来るようにしたシステムである。これは掲示板の管理者であっても掲示板への書き込みを行ったステーションであるクライアントＣＬを特定できなくしたもので、就職活動等を行う学生の企業への本音の意

見、採用面接に対するクレーム等を扱おうとしている。
システムの概要を図６に示す。ここでクライアントＣＬは学生、企業の担当者等、メール受付窓口となる機能サーバＦＳは学生の就職活動、企業の採用活動を支援する組織である。

【００５０】
ここで、公開掲示板Ｂに書き込む内容は、まず匿名にてメール受付窓口（機能サーバＦＳ）に送られる。さしさわりのない内容であればメール受付者はこれをメッセージ番号とともに公開掲示板Ｂに掲示する。次に、公開掲示板Ｂを見たユーザは、非公開の質問、反対意見等をメールとして公開されたメッセージ番号に対して送る。メール受付者はメッセージの内容に、さしさわりがなければこれを掲示するが、疑義がある場合は元のメッセージを送信したステーションに、匿名通信方式に基づいて通信サーバＣＳを経由して返信し、掲示は行わない。さらにメール受信者が、誹謗中傷メールと判断すれば返信も掲示も行わないものとする。
これにより、間に人間が介在するため、匿名性を悪用した悪意メールの掲示を防ぐことができる。

【００５１】
（応用例２）
本発明の第２の応用は電子投票システムへの応用である。大規模な電子投票のシステムとしてはブラインド署名による方法が有望であるが、この方法では通信の匿名性を別途確保する必要がある。本発明の匿名通信をブラインド署名と組み合わせれば、実用的な大規模電子投票システムが実現できる。図７に匿名通信方式を適用した電子投票方式の概要を示す。従来から提案されている方式は図中の実線矢印で示された以下の手順からなる。

【００５２】
（１）投票者は自らの投票内容を乱数でマスクした上で認証者に提出する（ルート３）。
（２）認証者は投票者を認証した上で、投票内容に署名を施して返送する（ルート４）。
（３）投票者は認証者から得た署名のマスクを取り外し、投票内容とともに投票管理者に提出する（ルート５）。
最後のステップ（ルート５）には匿名性が必要となるので、ここに本発明の方式を適用することができる。さらに本発明が実現する「匿名性を保ちつつ返信を受け取る」という機能によって、以下の点が改良される（図７の破線矢印を参照）。

【００５３】
（４）投票時に投票確認を受け取ることができる。
これによって、実際には投票を保留しながら締切後に「投票が受け付けられていない」と申し立てるような「投票の成立妨害」を防ぐことができる。投票結果の検証を締切後に行なえるため、投票の途中経過を公表する必要はなくなる（ルート６）。
また、投票集計に不正があった場合の投票者の対応としては、受け取った投票確認を何らかの方法で公開さえすればよく、投票の秘密を侵される危険が少ない（ルート７）。

【００５４】
（５）２重投票の検出において偶然による誤検出を避けるには、一意的な情報の振出しが必要になるが、本提案によれば、匿名性を保ちつつこれを実現できる（ルート１）と（ルート２）。

【００５５】
（応用例３）
本発明にかかる第３の応用は、インターネットなどの汎用回線に限定されるものではない。たとえば図５ではインターネットに適用する例としてＴＣＰヘッダを記載しているが、このことは必須条件ではない。たとえば、携帯電話のプロトコルなどへも原理的に応用可能であって、公開鍵、秘密鍵の組み合わせを利用することは、回線の種類に関係なく利用することが可能である。

【００５６】
（変形例）

本発明の骨子に寄れば、全てがネットワークで繋がれている必要はない。図８を例に説明する。基本的に図２と同じ構成であるが、違いは情報サーバＣＳ４に情報入力ターミナルＴ１が接続されている点であり、リスクは変わるが、機能サーバＦＳに情報ターミナルＴ２が接続されていても良い。

【００５７】

情報入力ターミナルＴ１若しくはＴ２は、オフライン用入力端末装置であって、フレキシブルディスク、メモリスティック、場合に寄ればキー入力など、情報提供者自らが訪れて提供したい情報とともに応答に必要な情報（図４でいえば、入力ターミナルＴ１の場合、秘匿アドレスＡＲ１、秘匿アドレスＡＲ３、秘匿アドレスＡＲ４の必要なアドレス情報。加えてメッセージＭＳ。情報サーバＣＬ４に繋がっているのでＡＲ２は必須ではない。）を入力するための端末装置である。

【００５８】

この方法は、キャッシュディスペンサのように人に見られないような管理された施設に設置され、例えば、最近設置されている「赤ちゃんポスト」のようなところで、置いていった主に匿名のまま応答が出来るようにするシステムが構築可能である。

【図面の簡単な説明】

【００５９】

【図１】従来のオニオンルーティングを利用した方法を説明するフローチャートである。

【図２】本発明のシステム構成を説明する図である。

【図３】本発明の匿名アドレスの匿名受け渡し原理を説明する図である。

【図４】本発明のデータ構造の例を説明する図である。

【図５】本発明を実施した処理時間の実施例の結果である。

【図６】本発明を公開掲示板へ適用する例の図である。

【図７】本発明を投票システムへ適用する例の図である。

【図８】本発明の変形例として、一部がオフライン化された図である。

【符号の説明】

【００６０】

ＣＬ　通信サーバにサブスクライバとして接続されたクライアント

ＣＬ１　送信元であるクライアント

ＦＳ　送信先となる機能サーバ（クライアントの一つ）

ＣＳ１　サブスクライバとしてクライアントを持つ通信サーバ１

ＣＳ２　サブスクライバとしてクライアントを持つ通信サーバ２

ＣＳ３　サブスクライバとしてクライアントを持つ通信サーバ３

ＣＳ４　サブスクライバとして機能サーバＦＳを含むクライアントを持つ通信サーバ４

ＣＳ５　サブスクライバとしてクライアントを持つ通信サーバ５

ＬＧ１　通信サーバ１に接続されるローカルグループ

ＬＧ２　通信サーバ２に接続されるローカルグループ

ＬＧ３　通信サーバ３に接続されるローカルグループ

ＬＧ４　通信サーバ４に接続されるローカルグループ

ＬＧ５　通信サーバ５に接続されるローカルグループ

ＬＮＷ　通信サーバがループ（リング）状に接続されたネットワーク（ループネットワーク）

Ｒ　ランダムビット列

ＦＳＯＫ　機能サーバＦＳの公開鍵

ＦＳＳＫ　機能サーバＦＳの秘密鍵

ＫＸ１　公開鍵ＦＳＯＫでＲを暗号化した符号列

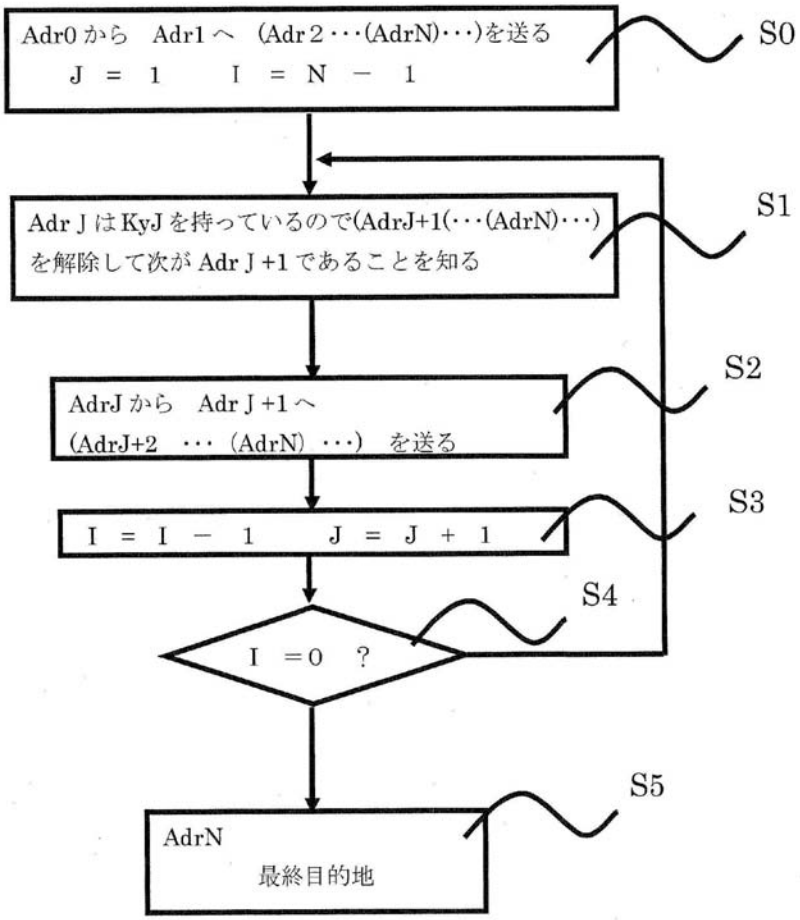
Ｈ　Ｒのハッシュ値

ＡＲ１　ＫＸ１とＨから成る機能サーバＦＳへ送るための、秘匿アドレス１（ＫＸ１，Ｈ）

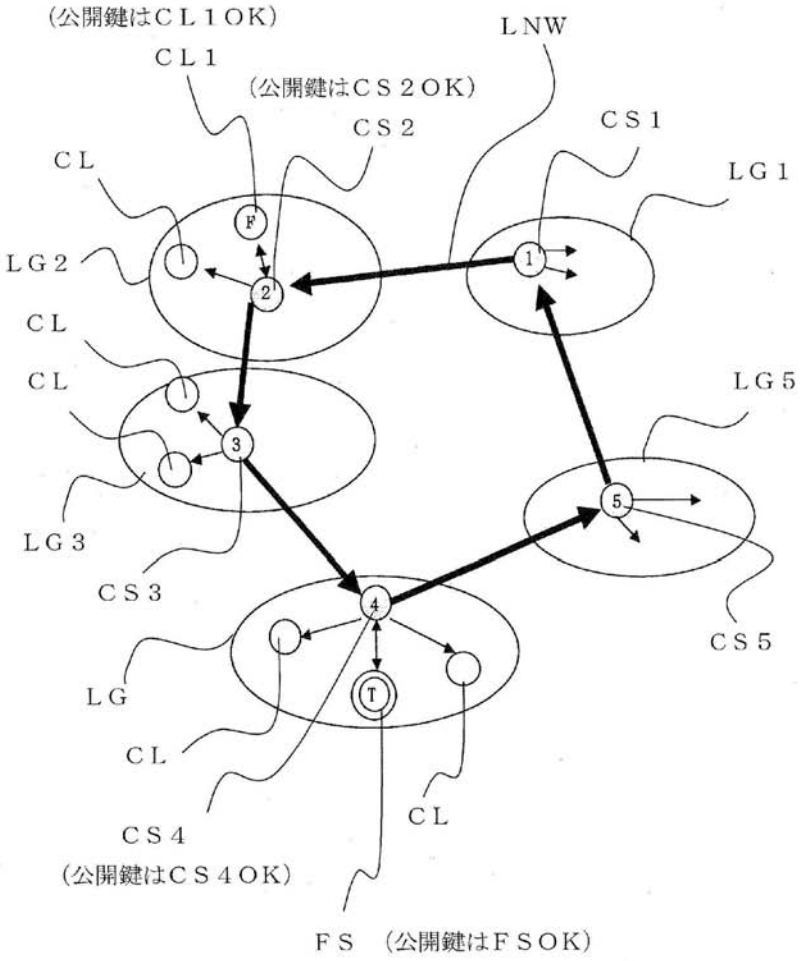
ＣＳＯＫ　通信サーバＣＳの公開鍵

ＣＳＯＫ　通信サーバＣＳの秘密鍵
ＣＳ４ＯＫ　通信サーバＣＳ４の公開鍵
ＣＳ４ＯＫ　通信サーバＣＳ４の秘密鍵
ＴＸ１　ＣＳ４ＯＫでＲを暗号化した符号列
ＡＲ２　ＴＸ１とＨから成る通信サーバＣＳ４へつなぐための、秘匿アドレス２（ＴＸ１，Ｈ）
ＣＬ１ＯＫ　クライアントＣＬ１の公開鍵
ＣＸ１　ＣＬ１ＯＫでＲを暗号化した符号列
ＡＲ３　機能サーバＦＳからクライアントＣＬ１へ応答するための秘匿アドレス３（ＣＸ１，Ｈ）
ＴＸ２　ＣＳ２ＯＫでＲを暗号化した符号列
ＡＲ４　機能サーバＦＳから通信サーバＣＳ２へ応答をつなぐための秘匿アドレス４（ＴＸ２、Ｈ）
ＭＳ　メッセージであって、ＴＣＰヘッダ、秘匿アドレス群、暗号化メッセージなどからなる
ＰＸ１　メッセージ本文を暗号化するパスワード
Ｂ　公開掲示板
Ｔ１　情報サーバに接続された情報入力ターミナル
Ｔ２　機能サーバに接続された情報入力ターミナル

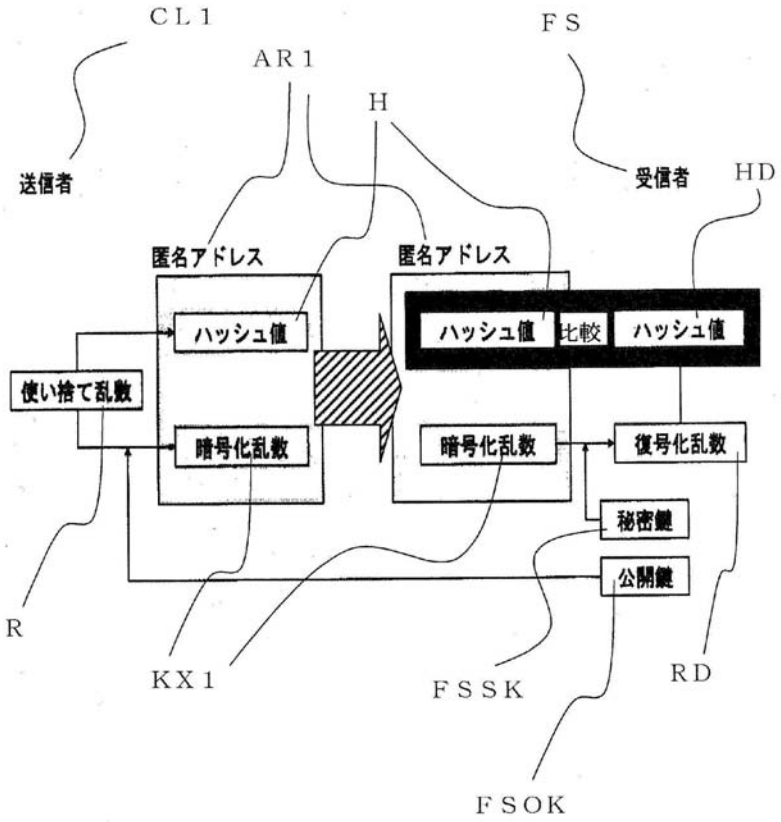
【図１】


Adr0 から Adr1 へ (Adr 2 ･･･(AdrN)･･･)を送る
J = 1 I = N − 1
S0
Adr J は KyJ を持っているので(AdrJ+1(･･･(AdrN)･･･)
を解除して次が Adr J +1 であることを知る
S1
AdrJ から Adr J +1 へ
(AdrJ+2 ･･･ (AdrN) ･･･) を送る
S2
I = I − 1 J = J + 1
S3
I =0 ?
S4
AdrN
最終目的地
S5

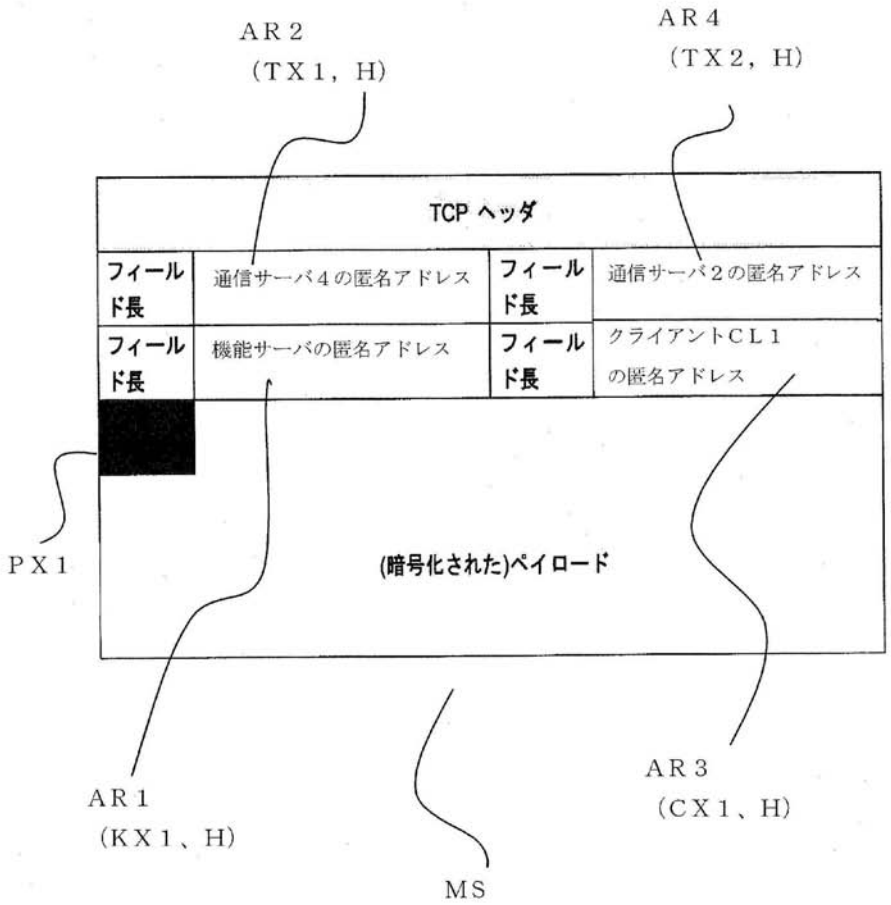
【図２】


（公開鍵はＣＬ１ＯＫ）
ＣＬ１
（公開鍵はＣＳ２ＯＫ）
ＣＳ２
ＬＮＷ
ＣＳ１
ＬＧ１
ＣＬ
ＬＧ２
ＣＬ
ＣＬ
ＬＧ５
ＬＧ３
ＣＳ３
ＣＳ５
ＬＧ
ＣＬ
ＣＬ
ＣＳ４
（公開鍵はＣＳ４ＯＫ）
ＦＳ （公開鍵はＦＳＯＫ）

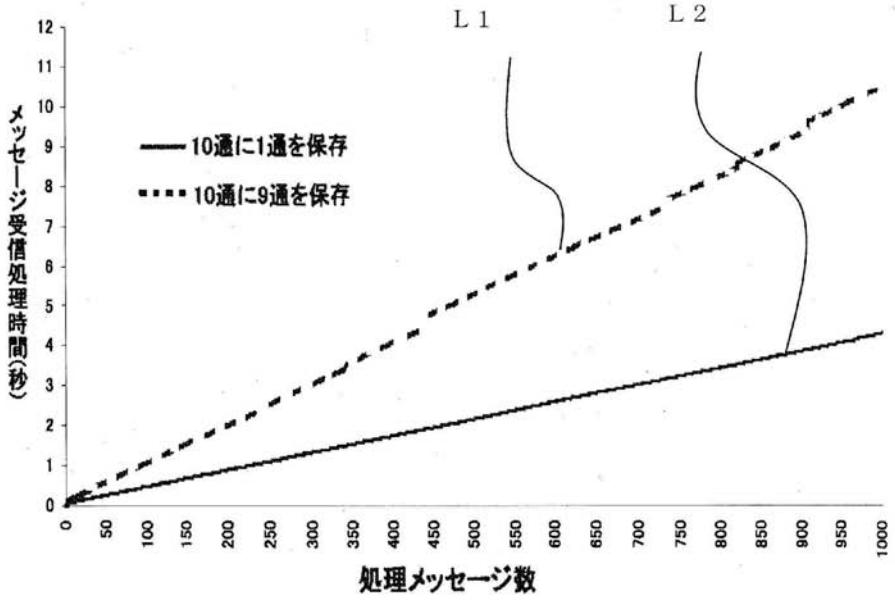
【図３】


CL1
AR1
H
FS
送信者
受信者
HD
匿名アドレス
匿名アドレス
ハッシュ値
ハッシュ値
比較
ハッシュ値
使い捨て乱数
暗号化乱数
暗号化乱数
復号化乱数
秘密鍵
公開鍵
R
KX1
FSSK
RD
FSOK

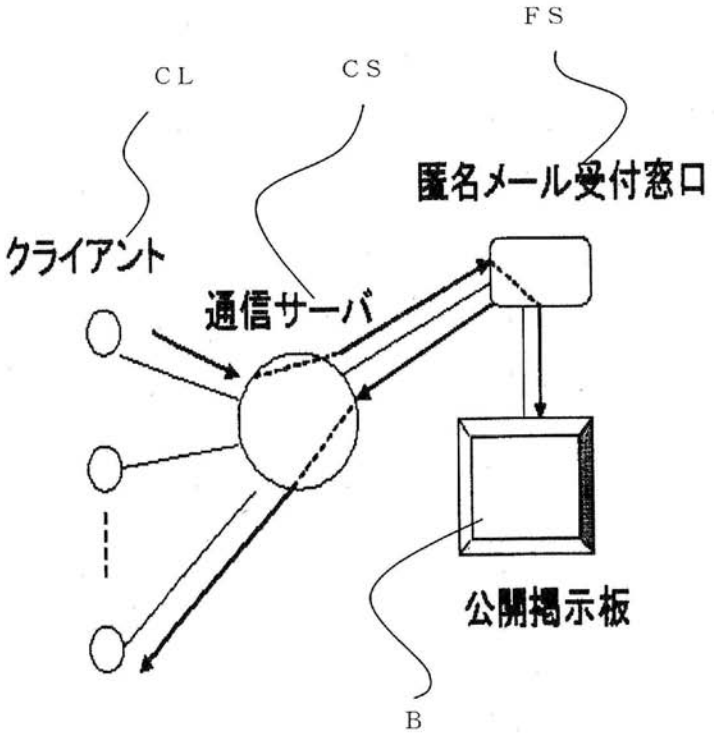
【図４】


ＡＲ２
（ＴＸ１，Ｈ）
ＡＲ４
（ＴＸ２，Ｈ）
TCP ヘッダ
フィールド長
通信サーバ４の匿名アドレス
フィールド長
通信サーバ２の匿名アドレス
フィールド長
機能サーバの匿名アドレス
フィールド長
クライアントＣＬ１
の匿名アドレス
ＰＸ１
(暗号化された)ペイロード
ＡＲ１
（ＫＸ１、Ｈ）
ＡＲ３
（ＣＸ１、Ｈ）
ＭＳ

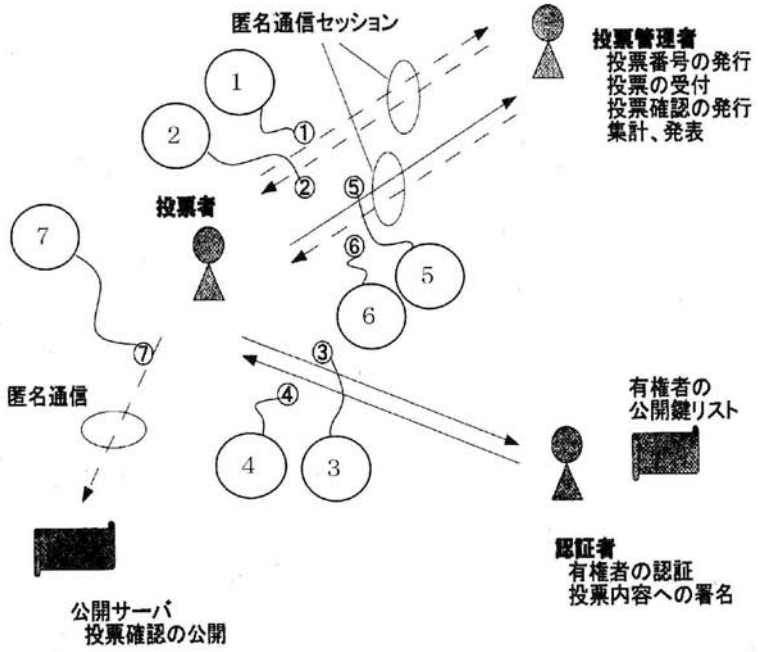
【図５】


L１
L２
10通に1通を保存
10通に9通を保存
メッセージ受信処理時間(秒)
処理メッセージ数
0
1
2
3
4
5
6
7
8
9
10
11
12
0
50
100
150
200
250
300
350
400
450
500
550
600
650
700
750
800
850
900
950
1000

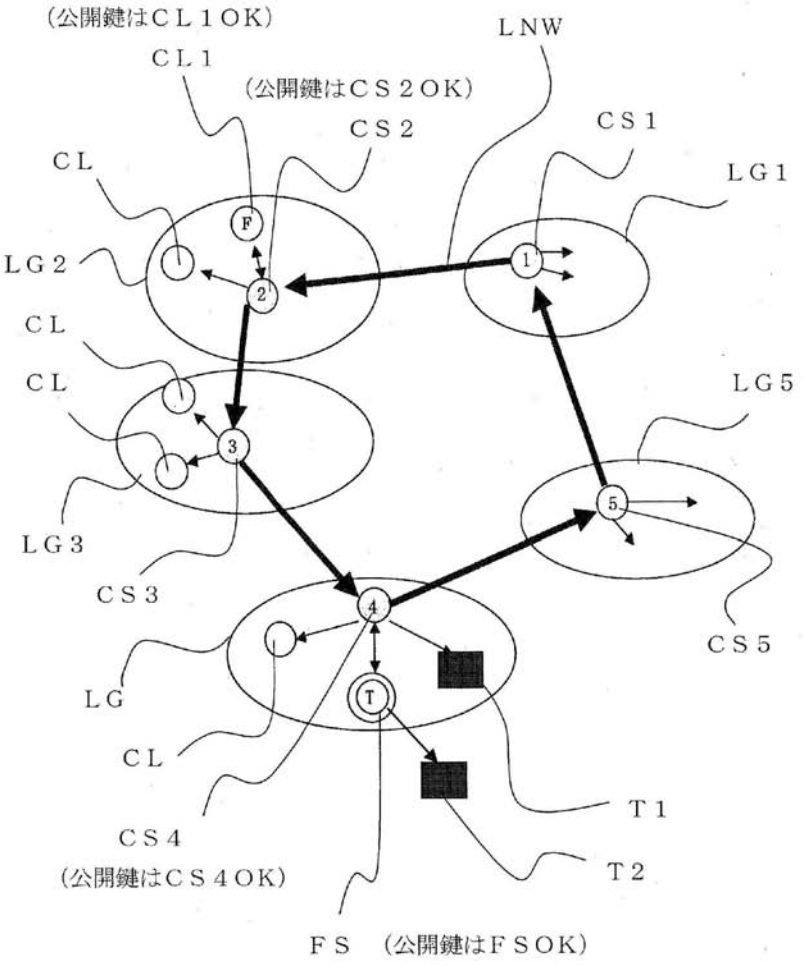
【図６】



【図７】


匿名通信セッション
投票管理者
投票番号の発行
投票の受付
投票確認の発行
集計、発表
投票者
匿名通信
有権者の
公開鍵リスト
認証者
有権者の認証
投票内容への署名
公開サーバ
投票確認の公開

【図８】


(公開鍵はＣＬ１ＯＫ)
ＣＬ１
(公開鍵はＣＳ２ＯＫ)
ＣＳ２
ＬＮＷ
ＣＳ１
ＬＧ１
ＣＬ
ＬＧ２
ＣＬ
ＣＬ
ＬＧ５
ＬＧ３
ＣＳ３
ＣＳ５
ＬＧ
ＣＬ
Ｔ１
ＣＳ４
(公開鍵はＣＳ４ＯＫ)
Ｔ２
ＦＳ　(公開鍵はＦＳＯＫ)