

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5211342号
(P5211342)

(45) 発行日 平成25年6月12日(2013.6.12)

(24) 登録日 平成25年3月8日(2013.3.8)

(51) Int.Cl. F I
H04L 9/32 (2006.01) H04L 9/00 675A

請求項の数 11 (全 20 頁)

| | | | |
|--------------|-------------------------------|-----------|---|
| (21) 出願番号 | 特願2008-211 (P2008-211) | (73) 特許権者 | 304023994 国立大学法人山梨大学 |
| (22) 出願日 | 平成20年1月4日(2008.1.4) | | 山梨県甲府市武田四丁目4番37号 |
| (65) 公開番号 | 特開2008-193667 (P2008-193667A) | (74) 代理人 | 100098589 弁理士 西山 善章 |
| (43) 公開日 | 平成20年8月21日(2008.8.21) | | |
| 審査請求日 | 平成22年6月9日(2010.6.9) | (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 |
| (31) 優先権主張番号 | 特願2007-5235 (P2007-5235) | (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 |
| (32) 優先日 | 平成19年1月12日(2007.1.12) | (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 |
| (33) 優先権主張国 | 日本国(JP) | | |

最終頁に続く

(54) 【発明の名称】 秘匿通信方法

(57) 【特許請求の範囲】

【請求項1】

予め設定されたルールに基づいてメッセージを回送するようにしたループネットワークに接続する複数の通信サーバの一の通信サーバの配下にある送信元クライアントと他の通信サーバの配下にある送信先クライアントとの間において送受信されるメッセージの秘匿通信方法であって、

前記送信元クライアントは、

生成されたランダムビット列のハッシュ値及び当該ランダムビット列を前記送信先クライアントの公開鍵を用いて暗号化した符合列を含む第1秘匿アドレス情報と、前記送信先クライアントが接続する通信サーバの公開鍵を用いて前記ランダムビット列を暗号化した符合列及びハッシュ値を含む第2秘匿アドレス情報と、を作成し、

少なくとも前記第1秘匿アドレス情報、前記第2秘匿アドレス及びメッセージ本文を含むメッセージを、前記一の通信サーバを介して前記ループネットワークに送出する、ことを特徴とするメッセージの秘匿通信方法。

【請求項2】

前記送信先クライアントが接続する通信サーバは、前記ループネットワークを介して回送されてくる前記メッセージにおける前記第2秘匿アドレス情報を自己の公開鍵に対応する秘密鍵を用いて復号化し、そのハッシュ値が一致した場合に自己の配下にある1又は複数のクライアントに送信し、

前記メッセージを受信したクライアントは、前記メッセージ中の前記第1秘匿アドレス

情報を自己の秘密鍵により復号化し、そのハッシュ値が一致した場合に当該メッセージが自己宛のメッセージであるとして受信する、ことを特徴とする請求項 1 に記載のメッセージの秘匿通信方法。

【請求項 3】

前記送信元クライアントは、さらに、

前記ランダムビット列を当該送信元クライアントの公開キーを用いて暗号化した符合列及び前記ハッシュ値を含む第 3 秘匿アドレス情報と、当該送信先クライアントが接続する通信サーバの公開キーを用いて前記ランダムビット列を暗号化した符合列及び前記ハッシュ値を含む第 4 秘匿アドレス情報と、を作成し、

前記送信先クライアント宛の前記メッセージに含ませて送信する、ことを特徴とする請求項 1 又は 2 に記載のメッセージの秘匿通信方法。

10

【請求項 4】

前記送信元クライアントから送信される前記メッセージのメッセージ本文は、前記送信先クライアントの公開鍵を用いて暗号化されたパスワードを含む暗号化送信文であって、

前記送信先クライアントは、自己の秘密鍵を用いて当該暗号化送信文を解読する、ことを特徴とする請求項 3 に記載のメッセージの秘匿通信方法。

【請求項 5】

前記送信元クライアントから送信されたメッセージを受信した前記送信先クライアントは、当該受信したメッセージの返信メッセージとして、

少なくとも前記第 3 秘匿アドレス情報、前記第 4 秘匿アドレス及び返信メッセージ本文を含む返信メッセージを、自己が接続する通信サーバを介して前記ループネットワークに送出する、ことを特徴とする請求項 3 に記載のメッセージの秘匿通信方法。

20

【請求項 6】

前記送信元クライアントが接続する通信サーバは、前記ループネットワークを介して回送されてくる前記返信メッセージにおける前記第 4 秘匿アドレス情報を自己の公開キーに対応する秘密鍵を用いて復号化し、そのハッシュ値が一致した場合に当該返信メッセージを自己の配下にある 1 又は複数のクライアントに転送し、

前記返信メッセージを受信した前記クライアントは、前記返信メッセージ中の前記第 3 秘匿アドレス情報を自己の秘密鍵により復号化し、そのハッシュ値が一致した場合に、当該返信メッセージが自己宛の返信メッセージであるとして受信する、ことを特徴とする請求項 5 に記載のメッセージの秘匿通信方法。

30

【請求項 7】

前記送信先クライアントから送信される前記返信メッセージのメッセージ本文は、前記送信元クライアントの公開鍵を用いて暗号化されたパスワードを含む暗号化送信文であり、

前記送信元クライアントは、自己の秘密鍵を用いて当該暗号化送信分を解読する、ことを特徴とする請求項 6 に記載のメッセージの秘匿通信方法。

【請求項 8】

前記複数の通信サーバの何れかに障害が発生した場合には、予め設定された他の通信サーバが、当該障害が発生した通信サーバの機能を代行する、ことを特徴とする請求項 1 乃至 7 の何れかに記載のメッセージの秘匿通信方法。

40

【請求項 9】

前記複数の通信サーバの各々は、回送されてきたメッセージが既に保持しているメッセージと一致している時には、当該メッセージが前記ループネットワークを一巡したものと判断して当該メッセージの回送を停止することを特徴とする請求項 8 に記載のメッセージの秘匿通信方法。

【請求項 10】

前記複数の通信サーバの各々は、受信したメッセージを配下にあるクライアントに転送した場合には、当該通信サーバに保持されていたメッセージを削除することを特徴とする請求項 8 に記載のメッセージの秘匿通信方法。

50

【請求項 1 1】

前記複数の通信サーバの各々とその配下にある前記クライアント間におけるメッセージの送受信は、ブロードキャスト通信又はオンデマンド通信である請求項 9 に記載のメッセージの秘匿通信方法。

【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。

10

【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。

20

【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。

インター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。

30

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。

40

【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。

50

【 0 0 0 7 】

ステップ S 1 の最初である $I = N - 1$ 、 $J = 1$ の状態では、宛先がアドレス $A d r 1$ のサーバであって、 $A d r 1$ サーバでは解除キー $K y 1$ を有しており、この $K y 1$ を用いて () を解除して $A d r 2$ が次ぎの宛先であること取得する。
そしてステップ S 2 で次の $A d r 2$ サーバに対して次のオニオンルーティング情報である ($A d r 3$ ($A d r 4 \cdots (A d r N) \cdots$)) を受け取った提供情報とともに送る。
ステップ S 3 とステップ S 4 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。

【 0 0 0 8 】

このように、以下順次 $A d r 3$ 、 $A d r 4$ へと送られてアドレス $A d r N$ の装置へ提供情報が伝達される。

このとき $A d r 1$ から $A d r N$ はそれぞれ解除キー $K y 1$ から $K y N$ 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 $A d r 0$ 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 2 0 0 4 - 2 2 9 0 7 1

【 発明の開示 】

【 発明が解決しようとする課題 】

【 0 0 0 9 】

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。

【 0 0 1 0 】

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 】

【 0 0 1 1 】

請求項 1 に記載の発明は、予め設定されたルールに基づいてメッセージを回送するようにしたループネットワークに接続する複数の通信サーバの一の通信サーバの配下にある送信元クライアントと他の通信サーバの配下にある送信先クライアントとの間において送受信されるメッセージの秘匿通信方法であって、前記送信元クライアントは、生成されたランダムビット列のハッシュ値及び当該ランダムビット列を前記送信先クライアントの公開鍵を用いて暗号化した符合列を含む第 1 秘匿アドレス情報と、前記送信先クライアントが接続する通信サーバの公開鍵を用いて前記ランダムビット列を暗号化した符合列及びハッシュ値を含む第 2 秘匿アドレス情報と、を作成し、少なくとも前記第 1 秘匿アドレス情報、前記第 2 秘匿アドレス及びメッセージ本文を含むメッセージを、前記一の通信サーバを介して前記ループネットワークに送出する、ことを特徴とするメッセージの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。

【 0 0 1 2 】

請求項 2 に記載の発明は、前記送信元クライアントは、前記ランダムビット列を当該送信元クライアントの公開鍵を用いて暗号化した符合列及び前記ハッシュ値を含む第 3 秘匿アドレス情報と、当該送信先クライアントが接続する通信サーバの公開鍵を用いて前記ランダムビット列を暗号化した符合列及び前記ハッシュ値を含む第 4 秘匿アドレス情報

10

20

30

40

50

と、を作成し、前記送信先クライアント宛の前記メッセージに含ませて送信する、ことを特徴とするものである。

【0013】

請求項3に記載の発明は、前記送信先クライアントが接続する通信サーバは、前記ループネットワークを介して回送されてくる前記メッセージにおける前記第2秘匿アドレス情報を自己の公開キーに対応する秘密鍵を用いて復号化し、そのハッシュ値が一致した場合に自己の配下にある1又は複数のクライアントに送信し、前記メッセージを受信したクライアントは、前記メッセージ中の前記第1秘匿アドレス情報を自己の秘密鍵により復号化し、そのハッシュ値が一致した場合に当該メッセージが自己宛のメッセージであるとして受信する、ことを特徴とするものである。

10

【0014】

請求項4に記載の発明は、前記送信元クライアントから送信される前記メッセージのメッセージ本文は、前記送信先クライアントの公開鍵を用いて暗号化されたパスワードを含む暗号化送信文であって、前記送信先クライアントは、自己の秘密鍵を用いて当該暗号化送信文を解読する、ことを特徴とするものである。

【0015】

請求項5に記載の発明は、前記送信元クライアントから送信されたメッセージを受信した前記送信先クライアントは、当該受信したメッセージの返信メッセージとして、少なくとも前記第3秘匿アドレス情報、前記第4秘匿アドレス及び返信メッセージ本文を含む返信メッセージを、自己が接続する通信サーバを介して前記ループネットワークに送出する、ことを特徴とするものである。

20

【0016】

請求項6に記載の発明は、前記送信元クライアントが接続する通信サーバは、前記ループネットワークを介して回送されてくる前記返信メッセージにおける前記第4秘匿アドレス情報を自己の公開キーに対応する秘密鍵を用いて復号化し、そのハッシュ値が一致した場合に当該返信メッセージを自己の配下にある1又は複数のクライアントに転送し、前記返信メッセージを受信した前記クライアントは、前記返信メッセージ中の前記第3秘匿アドレス情報を自己の秘密鍵により復号化し、そのハッシュ値が一致した場合に、当該返信メッセージが自己宛の返信メッセージであるとして受信する、ことを特徴とするものである。

30

【0017】

請求項7に記載の発明は、前記送信先クライアントから送信される前記返信メッセージのメッセージ本文は、前記送信元クライアントの公開鍵を用いて暗号化されたパスワードを含む暗号化送信文であり、前記送信元クライアントは、自己の秘密鍵を用いて当該暗号化送信分を解読する、ことを特徴とするものである。

【0018】

請求項8に記載の発明は、前記複数の通信サーバの何れかに障害が発生した場合には、予め設定された他の通信サーバが、当該障害が発生した通信サーバの機能を代行する、ことを特徴とするものである。

【0019】

請求項9に記載の発明は、前記複数の通信サーバの各々は、回送されてきたメッセージが既に保持しているメッセージと一致している時には、当該メッセージが前記ループネットワークを一巡したものと判断して当該メッセージの回送を停止することを特徴とするものである。

40

【0020】

請求項10に記載の発明は、前記複数の通信サーバの各々は、受信したメッセージを配下にあるクライアントに転送した場合には、当該通信サーバに保持されていたメッセージを削除することを特徴とするものである。

【0021】

そして、請求項11に記載の発明は、前記複数の通信サーバの各々とその配下にある前

50

記クライアント間におけるメッセージの送受信は、ブロードキャスト通信又はオンデマンド通信であることを特徴とするものである。

【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る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、自身のサブスクリ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）サブスクリバ：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

10

20

30

40

50

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及び自身の公開鍵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リ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。

10

【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。

20

(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】

30

(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。

40

【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FSK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

50

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を宛先として返信する。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と同様に使い捨てパスワード（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へ戻りたいので、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、ランダムビット列Rを受信者である機能サーバFSの公開鍵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

10

20

30

40

50

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バイト。

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 Dell Dimension1100(登録商標)

CPU Intel(登録商標)Pentium4(登録商標)

メモリ DDRSDRAM PC3200

OS UbuntuLinux7.04(登録商標)

NIC 100BASE-Tx/10BASE-T

ネットワーク(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。

10

20

30

40

50

【 0 0 4 9 】

(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 C L 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 C L 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 F S 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。

10

【 0 0 5 0 】

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 F S）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 C S 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。

20

【 0 0 5 1 】

(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。

【 0 0 5 2 】

(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）。

30

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）。

【 0 0 5 3 】

(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）。

40

【 0 0 5 4 】

(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）。

【 0 0 5 5 】

(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

50

。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。

10

【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、キャッシュディスク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。

20

【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。

30

【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 通信サーバにサブクライアント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 サブクライアントとしてクライアントを持つ通信サーバ1

CS2 サブクライアントとしてクライアントを持つ通信サーバ2

CS3 サブクライアントとしてクライアントを持つ通信サーバ3

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

40

CS5 サブクライアント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 通信サーバがグループ(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)

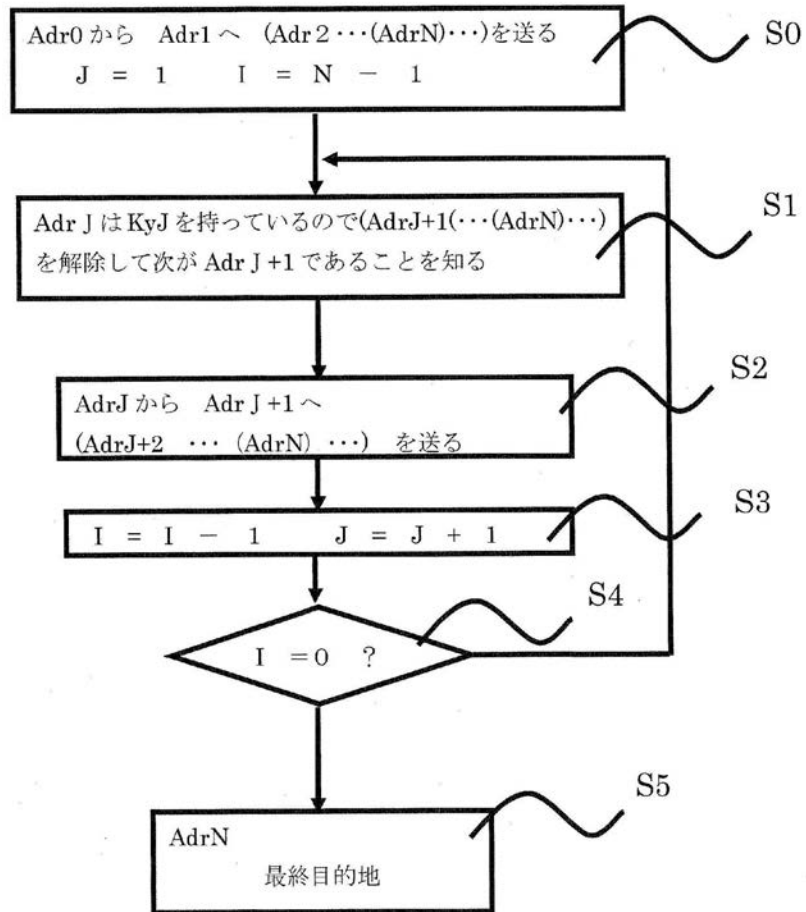
R ランダムビット列

FSOK 機能サーバFSの公開鍵

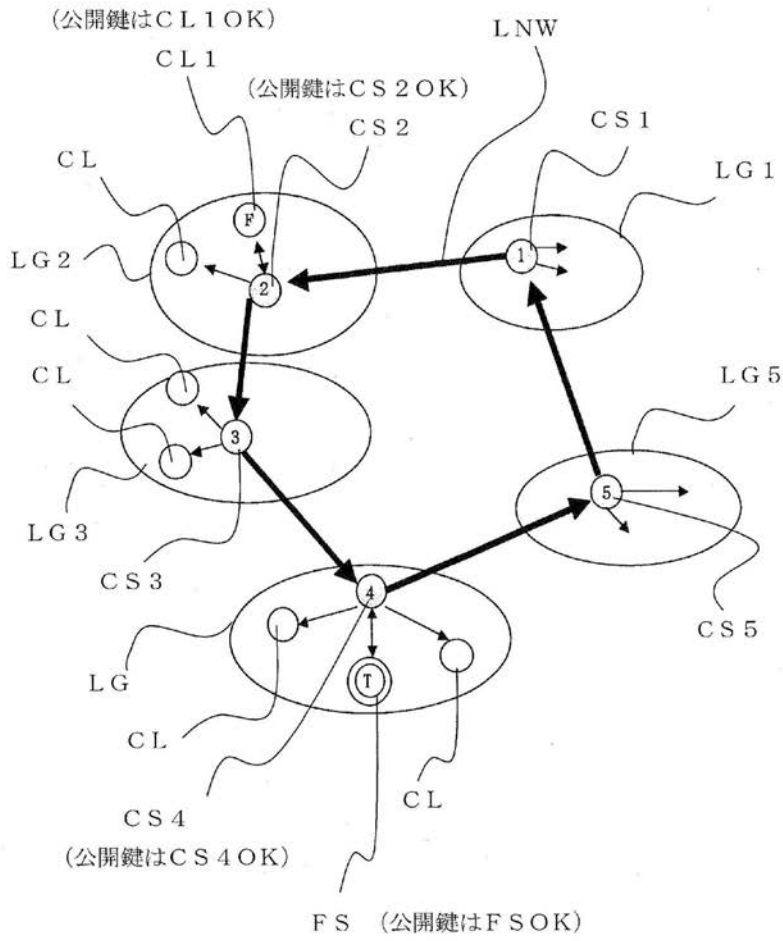
50

F S S K 機能サーバ F S の秘密鍵
 K X 1 公開鍵 F S O K で R を暗号化した符号列
 H R のハッシュ値
 A R 1 K X 1 と H から成る機能サーバ F S へ送るための、秘匿アドレス 1 (K X 1 , H)
 C S O K 通信サーバ C S の公開鍵
 C S O K 通信サーバ C S の秘密鍵
 C S 4 O K 通信サーバ C S 4 の公開鍵
 C S 4 O K 通信サーバ C S 4 の秘密鍵
 T X 1 C S 4 O K で R を暗号化した符号列 10
 A R 2 T X 1 と H から成る通信サーバ C S 4 へつなぐための、秘匿アドレス 2 (T X 1 , H)
 C L 1 O K クライアント C L 1 の公開鍵
 C X 1 C L 1 O K で R を暗号化した符号列
 A R 3 機能サーバ F S からクライアント C L 1 へ応答するための秘匿アドレス 3 (C X 1 , H)
 T X 2 C S 2 O K で R を暗号化した符号列
 A R 4 機能サーバ F S から通信サーバ C S 2 へ応答をつなぐための秘匿アドレス 4 (T X 2 , H)
 M S メッセージであって、 T C P ヘッダ、秘匿アドレス群、暗号化メッセージなどから 20
 なる
 P X 1 メッセージ本文を暗号化するパスワード
 B 公開掲示板
 T 1 情報サーバに接続された情報入力ターミナル
 T 2 機能サーバに接続された情報入力ターミナル

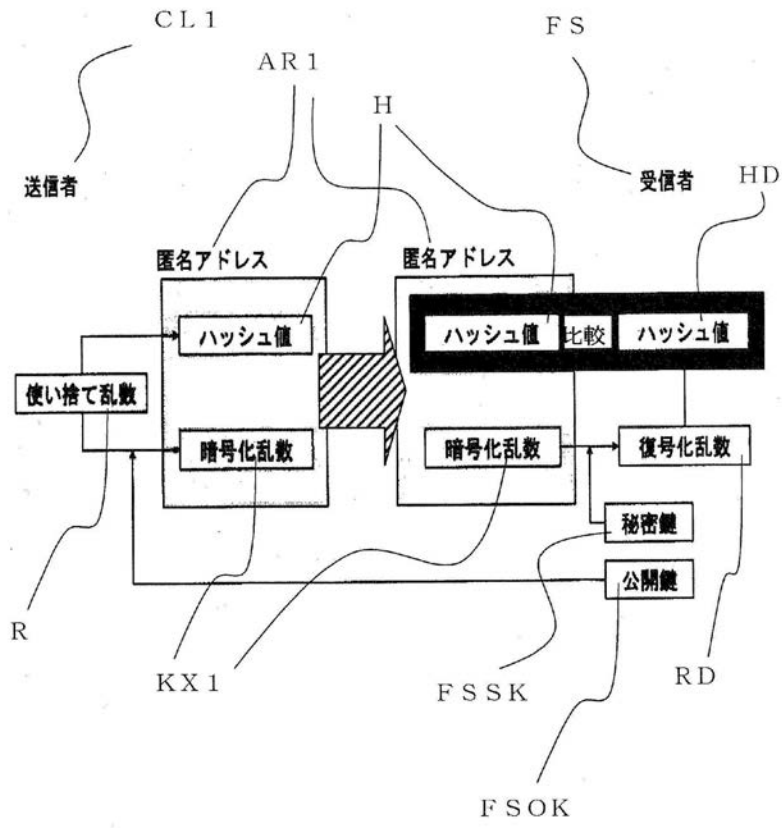
【図1】



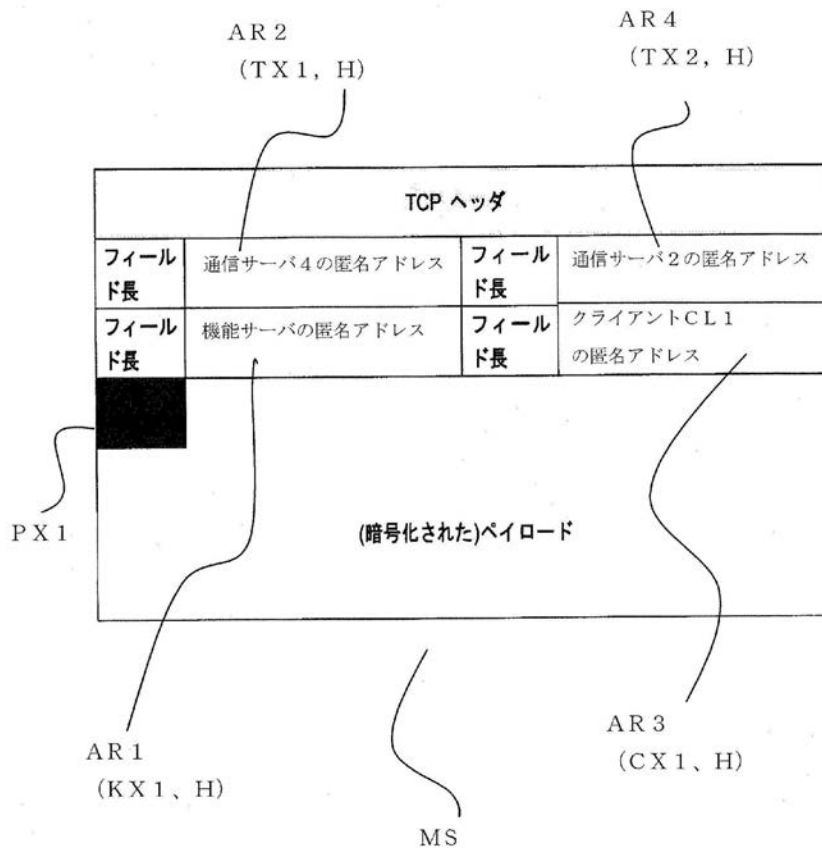
【図2】



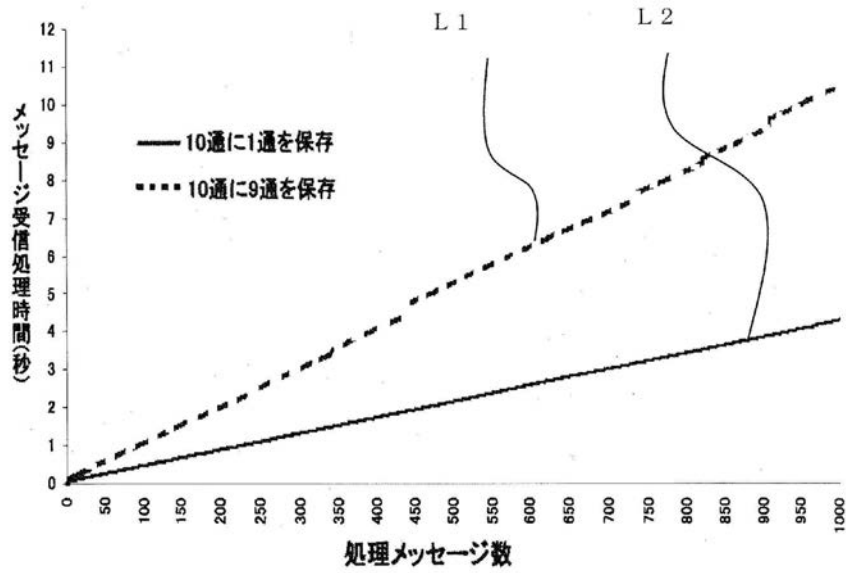
【図3】



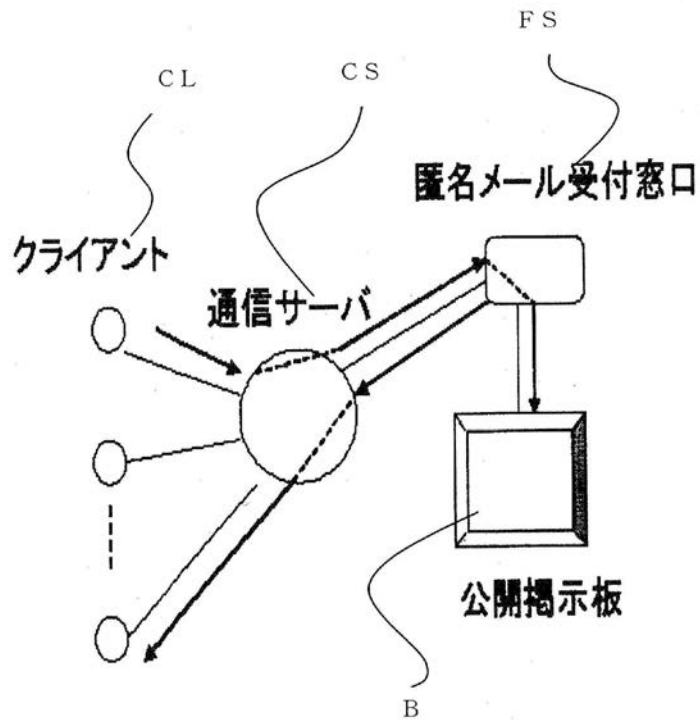
【図4】



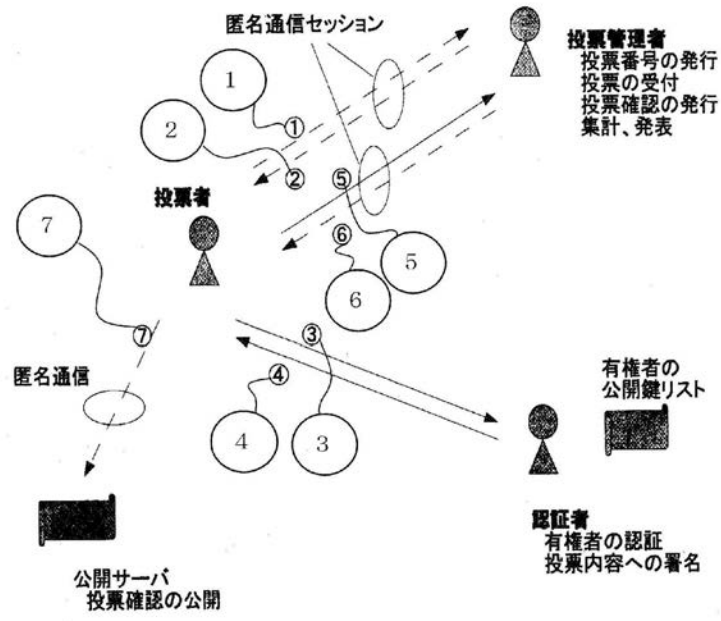
【 図 5 】



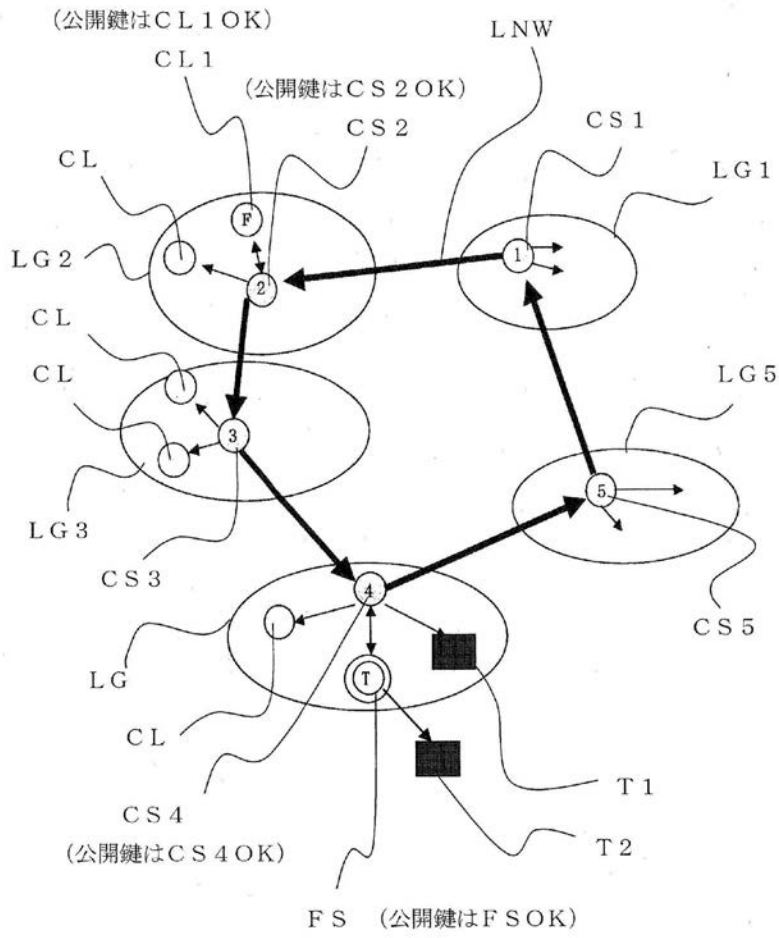
【 図 6 】



【図7】



【図8】



フロントページの続き

審査官 松平 英

- (56)参考文献 特開2001-147983(JP,A)
特開2003-078518(JP,A)
特開2005-159912(JP,A)
特開2005-167968(JP,A)
特開2006-295739(JP,A)
特開2006-304120(JP,A)
國米 仁 他, 個人情報を保護する匿名P2Pネットワーク基盤の開発, [online], 2003年, [平成24年10月17日検索], インターネット<URL: <http://www.ipa.go.jp/SPC/report/02fy-pro/index.htm>, <http://www.ipa.go.jp/SPC/report/02fy-pro/index.htm>>
田村 仁 他, 動的ネットワークにおける双方向匿名通信路構築手法の提案, 情報処理学会論文誌, 日本, 社団法人情報処理学会, 2007年 2月15日, 第48巻 第2号, p. 494~504

(58)調査した分野(Int.Cl., DB名)

H04L 9/00
G09C 1/00
G06F 21/20
G06F 21/24
H04L 12/00
H04L 29/00