(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2007-28606
(P2007-28606A)
(43)公開日　平成19年2月1日(2007.2.1)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/56	(2006.01)	H04L	12/56	A	5B285
H04L 12/66	(2006.01)	H04L	12/66	B	5J104
G06F 21/20	(2006.01)	G06F	15/00	330C	5K030
H04L 9/32	(2006.01)	H04L	9/00	673A	

審査請求 未請求　請求項の数 2　書面　（全 15 頁）

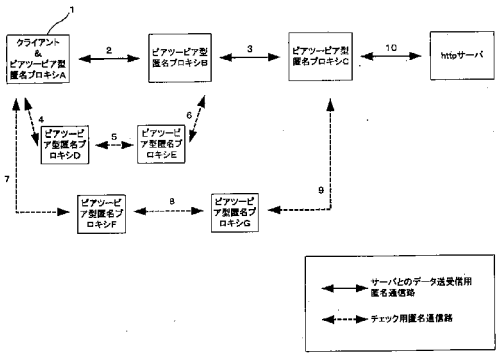
(21)出願番号　特願2006-184918 (P2006-184918)
(22)出願日　平成18年6月7日 (2006.6.7)
(62)分割の表示　特願2004-77168 (P2004-77168)の分割
原出願日　平成16年2月19日 (2004.2.19)

(71)出願人　504106000
西田　海
愛知県名古屋市千種区園山町２－３－１
園山スリーハウスＡ棟２０２号
(71)出願人　504209460
土方　嘉徳
大阪府豊中市待兼山町１－３　大阪大学大学院　基礎工学研究科内
(72)発明者　西田　海
愛知県名古屋市千種区園山町２－３－１
園山スリーハウスＡ棟２０２号
(72)発明者　土方　嘉徳
大阪府豊中市待兼山町１－３　大阪大学大学院　基礎工学研究科内

最終頁に続く

(54)【発明の名称】ピアツーピア型匿名プロキシにおける安全性の高い匿名通信路の検証及び構築する方法

(57)【要約】　（修正有）
【課題】信頼できる匿名通信路用サーバと信頼できない匿名通信路用サーバとが混在しているネットワークから、信頼性のある匿名通信路用サーバを選択し、安全性の高い匿名通信路の確保を可能とする。
【解決手段】ユーザが立ち上げている、自分及び他人が共同で使用できる匿名プロキシの性質を持った専用プログラム（以後、ピアツーピア型匿名プロキシと記載）から、他人が立ち上げているピアツーピア型匿名プロキシにアクセスし、サーバとのデータ送受信用匿名通信路を仮に構築する。この時、中継点となるピアツーピア型匿名プロキシから認証用のパスワードを受け取り、その後、新たに別の匿名通信路を構築し、その別の匿名通信路を用いて先ほどパスワードを受け取ったピアツーピア型匿名プロキシにアクセスし、パスワードの認証を行う。パスワードが一致すれば信頼できる中継点として確定され、その匿名通信路を用いてデータの送受信を行う。
【選択図】図１



【特許請求の範囲】
【請求項１】
ユーザが立ち上げている、自分及び他人が共同で使用できる匿名プロキシの性質を持った専用プログラム（以後、ピアツーピア型匿名プロキシと記載）から、他人が立ち上げているピアツーピア型匿名プロキシを用いて、サーバとのデータ送受信用匿名通信路を仮に構築し、各々の中継点となるピアツーピア型匿名プロキシからパスワードを受け取り、そのパスワードをピアツーピア型匿名プロキシで構築された別ルートのチェック用匿名通信路を通じて、仮に構築したデータ送受信用匿名通信路上のピアツーピア型匿名プロキシに該当すると思われるピアツーピア型匿名プロキシと送受信することでパスワード認証を行い、仮に構築したデータ送受信用匿名通信路上にあるピアツーピア型匿名プロキシを検証する工程と、上記パスワードを交換するために多重にデータを暗号化する工程を備えた通信方法。
【請求項２】
請求項１のサーバとのデータ送受信用匿名通信路の仮構築を行わず、データ送受信用匿名通信路を構築するピアツーピア型匿名プロキシの認証を、データ送受信用匿名通信路とは別ルートのピアツーピア型匿名プロキシで構築されたチェック用匿名通信路を用いて１つずつ検証し、データ送受信用匿名通信路を構築していく工程を備えた通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、コンピュータネットワークで安全性の高い匿名通信路を確保できる通信処理装置、通信方式、及びプログラムに関するものである。
【背景技術】
【０００２】
インターネットなどで使用されているＴＣＰ／ＩＰによる通信方法は、世の中でかなり普及している。この通信方法は、そのシンプルな構成から様々な機器でも対応しやすい規格になっている（図２）。
【０００３】
一般的に、インターネット上の通信データの大部分は暗号化されておらず、これらＩＰパケットの情報が中継となったコンピュータに丸見えの状態になっている。そのため、送信元と宛先の間の通信内容を、中継点となったコンピュータの悪意ある管理者がのぞき見することが可能である（図３）。
【０００４】
ＳＳＬなどの暗号化を施し通信した場合には、中継点の管理者がＩＰパケットを見ただけでは、そのデータ内容が分からないようになる。しかし、それ以外の情報であるＩＰヘッダやＴＣＰ／ＵＤＰヘッダに関しては暗号化されるわけではないので、中継となったコンピュータにどこからどこへ通信を行っているのか分かってしまう。
【０００５】
さらに、ＩＰ通信の手順上、情報をやり取りしたい通信相手である宛先に対しても、その送信元がどこなのか判明してしまうという欠点がある（図４の２０）。これを打破するためには、複数の匿名プロキシを中継点とし、これらの中継点を通して通信を行うことにより、送信元を宛先に知らせないということができる（図４の２２）。
【０００６】
しかし、この方法では全ての匿名プロキシの管理者に、通信の宛先がどこなのか分かってしまうという欠点がある。さらに、クライアントが一番最初に接続した匿名プロキシ（図４の２１）に対して、送信元と宛先の両方が露見してしまうという欠点がある。また、通信ルート自体が常に固定されるため、送信元が発覚しやすい。
【０００７】
このようなことを防ぐために特定の匿名プロキシを使用するのではなく、自分及び他人が共同で使用できる匿名プロキシの性質を持った専用プログラム（以後、ピアツーピア型

匿名プロキシと記載）を常に立ち上げ、これらの中から任意、もしくは無作為に中継点を選択し、見知らぬ人同士でピアツーピアの暗号通信を行いデータを相互に受け渡す匿名通信路を構築することにより、問題を解決することが可能となる（図５）。

【０００８】

この方法で、一番最初のピアツーピア型匿名プロキシは、自分で立ち上げているものであり信用できる。中継点となっているピアツーピア型匿名プロキシは、自分に接続してきた他のピアツーピア型匿名プロキシが、起点なのかそれとも他の中継点なのかネットワーク上のデータの流れからは判断できない。なぜなら、稼働しているピアツーピア型匿名プロキシは、通信の起点であると同時に他者の通信の中継点という２つの機能を有しているからである。ゆえに、外部からは判断が難しいものとなる。

【非特許文献１】ＲＦＣ７９１

【非特許文献２】ＲＦＣ９１９

【非特許文献３】ＲＦＣ９２２

【発明の開示】

【発明が解決しようとする課題】

【０００９】

図５のような方法で実際に通信することができれば、かなりの通信情報を漏洩させずに済むことができる。しかし、これはすべての中継点が正しく作動している場合であり、悪意ある改竄されたピアツーピア型匿名プロキシが中継点となった場合には、必ずしも安全に通信できるとは限らなくなる。具体的には、以下のような問題点が挙げられる。

【００１０】

お互いに接続しあっているピアツーピア型匿名プロキシ間の通信を、単純にＳＳＬなどの暗号通信した場合、ネットワークを外部から監視している第三者に対し、どれが接続元のクライアントになるピアツーピア型匿名プロキシなのかは把握されなくなる。しかし、これらの通信データはピアツーピア型匿名プロキシ内部にて内容の復号化を行うため、その中継となったピアツーピア型匿名プロキシの管理者には通信の宛先が分かってしまう。

【００１１】

また、中継点のピアツーピア型匿名プロキシが次の中継となるピアツーピア型匿名プロキシを決定するようにすると、お互い自分が中継となっている前後のＩＰアドレスしか把握できないようにすることが可能である。しかし、改竄されたピアツーピア型匿名プロキシが存在した場合には、より多くの中継点を通るようにユーザが指定していても、その通りにルーティングされなくなる可能性があり、匿名性が保たれるとは限らない。また、この場合に使っている匿名通信路が本当に安全なのか、ユーザ自身が確認する術がない。

【００１２】

逆に、ユーザ自身がどのようなルートを通るのか指定する場合には、正しくルーティングされているのかどうか確認できるが、中継点となっているピアツーピア型匿名プロキシにもそのルートが把握されてしまう。

【課題を解決するための手段】

【００１３】

匿名通信を行いたいユーザは、ユーザが使っているコンピュータでピアツーピア型匿名プロキシを立ち上げ（図１の１）、これを匿名通信路の起点とし、ピアツーピア型匿名プロキシＡとする。このピアツーピア型匿名プロキシＡは次の中継点となるピアツーピア型匿名プロキシＢを選択し、接続する。そして、お互いに公開鍵を交換する。ピアツーピア型匿名プロキシＢは認証用にユニークなパスワードを生成し、ピアツーピア型匿名プロキシＡ以外には知られないように暗号化してピアツーピア型匿名プロキシＡに送る（図１の２）。

【００１４】

ピアツーピア型匿名プロキシＡは、ピアツーピア型匿名プロキシＢの次の中継点ピアツーピア型匿名プロキシＣを選択し、ピアツーピア型匿名プロキシＢからピアツーピア型匿名プロキシＣに接続するようにする。ここでも、お互いに公開鍵を交換する。ピアツーピ

ア型匿名プロキシＣは認証用にユニークなパスワードを生成し、ピアツーピア型匿名プロキシＡ以外には知られないように暗号化してピアツーピア型匿名プロキシＡに送る（図１の２、３）。

【００１５】

ピアツーピア型匿名プロキシＡからピアツーピア型匿名プロキシＢとＣに接続したように、別ルートでピアツーピア型匿名プロキシＡからピアツーピア型匿名プロキシＤとＥに接続し、その後ピアツーピア型匿名プロキシＢにアクセスする。このとき、図１の２のルートにて取得したパスワードをピアツーピア型匿名プロキシＢ以外には知られないように暗号化してピアツーピア型匿名プロキシＢへ送り、認証を行う（図１の４、５、６）。

【００１６】

さらに、ピアツーピア型匿名プロキシＡからピアツーピア型匿名プロキシＢとＣに接続したように、別ルートでピアツーピア型匿名プロキシＡからピアツーピア型匿名プロキシＦとＧに接続し、その後ピアツーピア型匿名プロキシＣにアクセスする。このとき、図１の２、３のルートにて取得したパスワードをピアツーピア型匿名プロキシＣ以外には知られないように暗号化してピアツーピア型匿名プロキシＣへ送り、認証を行う（図１の７、８、９）。

【００１７】

ピアツーピア型匿名プロキシＢ及びピアツーピア型匿名プロキシＣとパスワードが一致した場合には、ピアツーピア型匿名プロキシＡが指定した通りの正しいルーティングが行われている証明になる。その後、図１の２、３、１０のルートを使い、ｈｔｔｐサーバなどにアクセスし、クライアントはサーバとデータの送受信を行う。このデータはピアツーピア型匿名プロキシＡまで暗号化されて送られ、中継となるピアツーピア型匿名プロキシにはその内容は一切把握されない（図１の２、３、１０、図５）。

【００１８】

また、サーバとのデータ送受信用匿名路の中継点になるピアツーピア型匿名プロキシを１つ１つ確認しながら構築する方法も考えられる。この場合には、図１の２、４、５、６、３、７、８、９、１０の順に接続されていくことになる。

【発明の効果】

【００１９】

通信相手（ｈｔｔｐサーバなど）に本来の送信元を知らせることなく、通信することが可能になる。また、終点のピアツーピア型匿名プロキシ以外に通信の宛先が分からない。そのため、会社やプロバイダなどのユーザがインターネットに接続するにあたって属している組織に対しても、通信の宛先を秘匿することができる。終点のピアツーピア型匿名プロキシ以外に通信相手（ｈｔｔｐサーバなど）とのパケット内容が一切分からない。ユーザが立ち上げ起点となるピアツーピア型匿名プロキシ以外の匿名通信路を構成する中継点のピアツーピア型匿名プロキシには、通信の本来の送信元がどこであるのか分からない。送信元と宛先を秘匿したままで、既存のｈｔｔｐやｆｔｐなどのＴＣＰやＵＤＰを使用したインターネットサービスをそのまま利用することができる。

【００２０】

ピアツーピア型匿名プロキシの中継点に、その接続ルートの前後しか把握できないようにし、かつユーザが指定した通りのルーティングが行われているのか、確認することができる。そのため、信頼できない中継点が存在している場合にも、それらを排除して匿名通信路を形成することが可能になる。

【００２１】

ユーザ自身も匿名通信路用にピアツーピア型匿名プロキシを立ち上げることになるため、匿名通信路を使用するユーザが増加しても、その分中継点となるピアツーピア型匿名プロキシが増えるので回線の速度低下を免れやすい。また、匿名通信路を確保するにあたって、そのピアツーピア型匿名プロキシ間の速度を考慮して匿名通信路を選択することにより、常に空いているネットワークを効率よく利用して接続することが可能になる。

【発明を実施するための最良の形態】

【００２２】
状況に応じて、２種類の方法が考えられる。図１の２、３、４、５、６、７、８、９、１０の順に接続する形式は、信頼できる中継点が多い場合に適した接続方法である。なぜなら、４、５、６と７、８、９のルートを同時にアクセスすることが可能だからである。図１の２、４、５、６、３、７、８、９、１０の順に接続する形式は、信頼できない中継点が多い場合に適した接続方法である。なぜなら、一度にサーバとのデータ送受信用匿名通信路を構築しても、その後の検証で不正なピアツーピア型匿名プロキシの存在が発覚した場合に、そのサーバとのデータ送受信用匿名通信路の構築を最初からやり直さなくてはいけないからである。これらは、サーバとのデータ送受信用匿名通信路とチェック用匿名通信路の確立順序が異なるだけで、基本的なやり取りは同じである。そのため、実施例では前者の説明を行う。

【実施例】

【００２３】
図６は、匿名通信路を構築するフローチャートを示している。ｈｔｔｐサーバ等のサーバＳＶへアクセスしたいユーザＵ０は、事前にピアツーピア型匿名プロキシのＰ（Ｕ０）を立ち上げておく。その後、ユーザＵ０はいくつのピアツーピア型匿名プロキシを中継点として通すのかというＰ（Ｕ０）の内部変数ｍを決定しておく（ステップＳ１）。その後、Ｐ（Ｕ０）は、内部で保持している他のピアツーピア型匿名プロキシのＩＰアドレス一覧からランダムに１つアドレスを選択する（ステップＳ２）。この選択されたＩＰアドレスはＡ（Ｕ１）で、Ｐ（Ｕ０）の次の中継点となる。Ｐ（Ｕ０）は現在中継してるピアツーピア型匿名プロキシの数を示す内部変数ｎを０で初期化する（ステップＳ３）。

【００２４】
ｎ＝０の場合（ステップＳ４）に、Ｐ（Ｕ０）は公開鍵ＬＰ１（Ｕ０）とそれに対応する秘密鍵ＬＳ１（Ｕ０）、及び公開鍵ＬＰ２（Ｕ０）とそれに対応する秘密鍵ＬＳ２（Ｕ０）を生成する（ステップＳ５）。

【００２５】
Ｐ（Ｕｎ）は、ＩＰアドレスがＡ（Ｕｎ＋１）であるＰ（Ｕｎ＋１）と接続する（ステップＳ６）。Ｐ（Ｕｎ＋１）は、公開鍵ＬＰ１（Ｕｎ＋１）とそれに対応する秘密鍵ＬＳ１（Ｕｎ＋１）を生成する（ステップＳ７）。そして、Ｐ（Ｕｎ＋１）からＰ（Ｕｎ）へ暗号化せず、公開鍵ＬＰ１（Ｕｎ＋１）を送る（ステップＳ８）。Ｐ（Ｕｎ）はそのデータを受け取る。

【００２６】
Ｐ（Ｕ０）にて変数ｎが０でない場合（ステップＳ９）、Ｐ（Ｕｎ）からＰ（Ｕ０）へ公開鍵ＬＰ２（Ｕ０）で暗号化し、公開鍵ＬＰ１（Ｕｎ＋１）を送る。Ｐ（Ｕ０）は受け取ったデータを秘密鍵ＬＳ２（Ｕ０）で復号化する（ステップＳ１０）。このとき、Ｐ（Ｕｎ）からＰ（Ｕ０）へは直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｕｎ）からＰ（Ｕｎ－１）へ、Ｐ（Ｕｎ－１）からＰ（Ｕｎ－２）へ、という順でＰ（Ｕ０）へ送る（図７）。

【００２７】
図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｕｎ）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図６のステップＳ１０の公開鍵ＬＰ２（Ｕ０）で暗号化した公開鍵ＬＰ１（Ｕｎ＋１）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｕ０）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｕｎ－ｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｕｎ－ｋ－１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｕｎ－ｋ－１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｕ０）が一致する場合（ステップＳ３４）、図６のステップＳ１１に飛ぶ。

【００２８】
Ｐ（Ｕｎ）からＰ（Ｕｎ＋１）へ公開鍵ＬＰ１（Ｕｎ＋１）で暗号化し、公開鍵ＬＰ１（Ｕｎ）と公開鍵ＬＰ２（Ｕ０）を送る。Ｐ（Ｕｎ＋１）は、受け取ったデータを秘密鍵ＬＳ１（Ｕｎ＋１）で復号化する（ステップＳ１１）。
【００２９】
Ｐ（Ｕｎ＋１）はユニークなパスワードＰＷ（Ｕｎ＋１）を生成する（ステップＳ１２）。Ｐ（Ｕｎ＋１）からＰ（Ｕ０）へ公開鍵ＬＰ２（Ｕ０）で暗号化し、パスワードＰＷ（Ｕｎ＋１）を送る。Ｐ（Ｕ０）は、受け取ったデータを秘密鍵ＬＳ２（Ｕ０）で復号化する（ステップＳ１３）。このとき、Ｐ（Ｕｎ＋１）からＰ（Ｕ０）へ直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｕｎ＋１）からＰ（Ｕｎ）へ、Ｐ（Ｕｎ）からＰ（Ｕｎ－１）へ、という順でＰ（Ｕ０）へ送る（図７）。
【００３０】
図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｕｎ＋１）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図６のステップＳ１３の公開鍵ＬＰ２（Ｕ０）で暗号化したユニークなパスワードＰＷ（Ｕｎ＋１）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｕ０）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｕｎ＋１－ｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｕｎ－ｋ）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｕｎ－ｋ）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｕ０）が一致する場合（ステップＳ３４）、図６のステップＳ１４に飛ぶ。
【００３１】
Ｐ（Ｕ０）は、ｍ＝ｎ＋１が成立するか確認する。成立する場合には、ステップＳ１８へ飛び、成立しない場合には、ステップＳ１５へ飛ぶ（ステップＳ１４）。Ｐ（Ｕ０）は、内部で保持している他のピアツーピア型匿名プロキシのＩＰアドレス一覧からランダムに１つ選択する（ステップＳ１５）。この選択されたＩＰアドレスはＡ（Ｕｎ＋２）で、Ｐ（Ｕｎ＋１）の次の中継点となる。Ｐ（Ｕ０）からＰ（Ｕｎ＋１）へ公開鍵ＬＰ１（Ｕｎ＋１）で暗号化し、ＩＰアドレスＡ（Ｕｎ＋２）を送る。Ｐ（Ｕｎ＋１）は受け取ったデータを秘密鍵ＬＳ１（Ｕｎ＋１）で復号化する（ステップＳ１６）。このとき、Ｐ（Ｕ０）からＰ（Ｕｎ＋１）へは直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｕ０）からＰ（Ｕ１）へ、Ｐ（Ｕ１）からＰ（Ｕ２）へ、という順でＰ（Ｕｎ＋１）へ送る（図７）。
【００３２】
図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｕ０）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図６のステップＳ１６の公開鍵ＬＰ１（Ｕｎ＋１）で暗号化したＩＰアドレスＡ（Ｕｎ＋２）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｕｎ＋１）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｕｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｕｋ＋１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｕｋ＋１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｕｎ＋１）が一致する場合（ステップＳ３４）、図６のステップＳ１７に飛ぶ。
【００３３】
Ｐ（Ｕ０）はｎに１を加算し、ステップＳ４へ飛ぶ（ステップＳ１７）。
【００３４】
Ｐ（Ｕ０）は、内部変数ｎを１に初期化する（ステップＳ１８）。Ｐ（Ｕ０）からＰ（

Ｕｎ）へ接続し、ステップＳ１３で受け取ったパスワードをＰ（Ｕｎ）へ送り、またＰ（Ｕｎ）から同一パスワードもしくは返値を受け取る（ステップＳ１９、図８）。

【００３５】

図８のフローチャートについて説明する。図８のステップＳ３７からＳ５３までは、図６のステップＳ１からステップＳ１７までとほぼ同じ流れとなる。Ｃ０とＵ０は同一のユーザであり、ピアツーピア型匿名プロキシのＰ（Ｃ０）はＰ（Ｕ０）と同一のものである。また、ｎ＞０、ｉ＞０の場合、ＵｎとＣｉは全て異なるユーザであり、Ｐ（Ｕｎ）、Ｐ（Ｃｉ）も全て異なるピアツーピア型匿名プロキシである。ここで、Ｐ（Ｕｎ）へアクセスしたいユーザＣ０（＝Ｕ０）は、事前にいくつのピアツーピア型匿名プロキシを中継点として通るのかというＰ（Ｕ０）の内部変数ｈを決定しておく（ステップＳ３７）。その後、ユーザＣ０が立ち上げているピアツーピア型匿名プロキシのＰ（Ｃ０）（＝Ｐ（Ｕ０））は、内部で保持している他のピアツーピア型匿名プロキシのＩＰアドレス一覧からランダムに１つアドレスを選択する（ステップＳ３８）。この選択されたＩＰアドレスはＡ（Ｃ１）で、Ｐ（Ｃ０）の次の中継点となる。Ｐ（Ｕ０）は内部変数ｉを０で初期化する（ステップＳ３９）。

【００３６】

ｉ＝０の場合（ステップＳ４０）に、Ｐ（Ｃ０）は公開鍵ＬＰ３（Ｃ０）とそれに対応する秘密鍵ＬＳ３（Ｃ０）、及び公開鍵ＬＰ４（Ｃ０）とそれに対応する秘密鍵ＬＳ４（Ｃ０）を生成する（ステップＳ４１）。

【００３７】

Ｐ（Ｃｉ）は、ＩＰアドレスがＡ（Ｃｉ＋１）であるＰ（Ｃｉ＋１）と接続する（ステップＳ４２）。Ｐ（Ｃｉ＋１）は、公開鍵ＬＰ３（Ｃｉ＋１）とそれに対応する秘密鍵ＬＳ３（Ｃｉ＋１）を生成する（ステップＳ４３）。そして、Ｐ（Ｃｉ＋１）からＰ（Ｃｉ）へ暗号化せず、公開鍵ＬＰ３（Ｃｉ＋１）を送る（ステップＳ４４）。Ｐ（Ｃｉ）はそのデータを受け取る。

【００３８】

Ｐ（Ｃ０）にて変数ｉが０でない場合（ステップＳ４５）、Ｐ（Ｃｉ）からＰ（Ｃ０）へ公開鍵ＬＰ４（Ｃ０）で暗号化し、公開鍵ＬＰ３（Ｃｉ＋１）を送る。Ｐ（Ｃ０）は受け取ったデータを秘密鍵ＬＳ４（Ｃ０）で復号化する（ステップＳ４６）。このとき、Ｐ（Ｃｉ）からＰ（Ｃ０）へは直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｃｉ）からＰ（Ｃｉ－１）へ、Ｐ（Ｃｉ－１）からＰ（Ｃｉ－２）へ、という順でＰ（Ｃ０）へ送る（図７）。

【００３９】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｃｉ）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図８のステップＳ４６の公開鍵ＬＰ４（Ｃ０）で暗号化した公開鍵ＬＰ３（Ｃｉ＋１）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｃｉ－ｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｃｉ－ｋ－１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ３（Ｃｉ－ｋ－１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致する場合（ステップＳ３４）、図８のステップＳ４７に飛ぶ。

【００４０】

Ｐ（Ｃｉ）からＰ（Ｃｉ＋１）へ公開鍵ＬＰ３（Ｃｉ＋１）で暗号化し、公開鍵ＬＰ３（Ｃｉ）と公開鍵ＬＰ４（Ｃ０）を送る。Ｐ（Ｃｉ＋１）は、受け取ったデータを秘密鍵ＬＳ３（Ｃｉ＋１）で復号化する（ステップＳ４７）。

【００４１】

Ｐ（Ｃｉ＋１）はユニークなパスワードＰＷ（Ｃｉ＋１）を生成する（ステップＳ４８

）。Ｐ（Ｃｉ＋１）からＰ（Ｃ０）へ公開鍵ＬＰ４（Ｃ０）で暗号化し、パスワードＰＷ（Ｃｉ＋１）を送る。ただし、現在の経路は図１のチェック用匿名通信路であるため、このパスワードが使われることはない。中継となっているピアツーピア型匿名プロキシに対し、データ送受信用匿名通信路か、チェック用匿名通信路か判断されないためにパスワードを送る処理を行っている。Ｐ（Ｃ０）は、受け取ったデータを秘密鍵ＬＳ４（Ｃ０）で復号化する（ステップＳ４９）。このとき、Ｐ（Ｃｉ＋１）からＰ（Ｃ０）へ直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｃｉ＋１）からＰ（Ｃｉ）へ、Ｐ（Ｃｉ）からＰ（Ｃｉ－１）へ、という順でＰ（Ｃ０）へ送る（図７）。

【００４２】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｃｉ＋１）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図８のステップＳ４９の公開鍵ＬＰ４（Ｃ０）で暗号化したユニークなパスワードＰＷ（Ｃｉ＋１）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｃｉ＋１－ｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｃｉ－ｋ）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ３（Ｃｉ－ｋ）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致する場合（ステップＳ３４）、図８のステップＳ５０に飛ぶ。

【００４３】

Ｐ（Ｃ０）は、ｈ＝ｉ＋１が成立するか確認する。成立する場合には、ステップＳ５４へ飛び、成立しない場合には、ステップＳ５１へ飛ぶ（ステップＳ５０）。Ｐ（Ｃ０）は、内部で保持している他のピアツーピア型匿名プロキシのＩＰアドレス一覧からランダムに１つ選択する（ステップＳ５１）。この選択されたＩＰアドレスはＡ（Ｃｉ＋２）で、Ｐ（Ｃｉ＋１）の次の中継点となる。Ｐ（Ｃ０）からＰ（Ｃｉ＋１）へ公開鍵ＬＰ３（Ｃｉ＋１）で暗号化し、ＩＰアドレスＡ（Ｃｉ＋２）を送る。Ｐ（Ｃｉ＋１）は受け取ったデータを秘密鍵ＬＳ３（Ｃｉ＋１）で復号化する（ステップＳ５２）。このとき、Ｐ（Ｃ０）からＰ（Ｃｉ＋１）へは直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｃ０）からＰ（Ｃ１）へ、Ｐ（Ｃ１）からＰ（Ｃ２）へ、という順でＰ（Ｃｉ＋１）へ送る（図７）。

【００４４】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｃ０）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図８のステップＳ５２の公開鍵ＬＰ３（Ｃｉ＋１）で暗号化したＩＰアドレスＡ（Ｃｉ＋２）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｃｉ＋１）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｃｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｃｋ＋１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ３（Ｃｋ＋１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｃｉ＋１）が一致する場合（ステップＳ３４）、図８のステップＳ５３に飛ぶ。

【００４５】

Ｐ（Ｃ０）はｉに１を加算し、ステップＳ４０へ飛ぶ（ステップＳ５３）。

【００４６】

Ｐ（Ｃ０）からＰ（Ｕｎ）へ公開鍵ＬＰ１（Ｕｎ）で暗号化し、図６のステップＳ１３で受け取ったパスワードＰＷ（Ｕｎ）を送る。Ｐ（Ｕｎ）は受け取ったデータを秘密鍵ＬＳ１（Ｕｎ）で復号化する（ステップＳ５４）。このとき、Ｐ（Ｃ０）からＰ（Ｕｎ）へ

は直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｃ０）からＰ（Ｃ１）へ、Ｐ（Ｃ１）からＰ（Ｃ２）へ、という順でＰ（Ｕｎ）へ送る（図７）。

【００４７】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｃ０）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図８のステップＳ５４の公開鍵ＬＰ１（Ｕｎ）で暗号化したパスワードＰＷ（Ｕｎ）に相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｕｎ）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｕｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｕｋ＋１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｕｋ＋１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致する場合（ステップＳ３４）、図８のステップＳ５５に飛ぶ。

【００４８】

Ｐ（Ｕｎ）は復号化したデータを過去の特定時間内にＰ（Ｕｎ）が生成したパスワード群と一致するか確認する。一致した場合には、Ｐ（Ｕｎ）からＰ（Ｃ０）へ公開鍵ＬＰ２（Ｕ０）で暗号化し、パスワードＰ（Ｕｎ）を送り返す。Ｐ（Ｃ０）から送られてきたデータが復号化できない場合や、パスワードが一致しない場合はそれを伝える内容をＰ（Ｃ０）へ送り返す。Ｐ（Ｃ０）は受け取ったデータを秘密鍵ＬＳ２（Ｕ０）で復号化する（ステップＳ５５）。このとき、Ｐ（Ｕｎ）からＰ（Ｃ０）へ直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｕｎ）からＰ（Ｃｈ）へ、Ｐ（Ｃｈ）からＰ（Ｃｈ－１）へ、という順でＰ（Ｕｎ）へ送る（図７）。

【００４９】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｕｎ）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図８のステップＳ５５の公開鍵ＬＰ２（Ｕ０）で暗号化したパスワードＰＷ（Ｕｎ）に相当し、Ｐ（Ｕｎ）でパスワードが一致しなかった場合にはそれを伝える内容に相当する。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、ｋ＝０の時、Ｐ（Ｒｋ）はＰ（Ｕｎ）に、ｋ＞０のときＰ（Ｒｋ）はＰ（Ｃｈ＋１－ｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｃｈ－ｋ）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｃｈ－ｋ）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｃ０）が一致する場合（ステップＳ３４）、図６のステップＳ２０に飛ぶ。

【００５０】

Ｐ（Ｕ０）は、Ｐ（Ｕｎ）から送り返されてきたデータを秘密鍵ＬＳ２（Ｕ０）で復号化する（ステップＳ５５）が、この時にデータを正しく復号化できなかったり、データがパスワードＰＷ（Ｕｎ）と異なる場合（ステップＳ２０）には、データ送受信用匿名通信路においてＰ（Ｕ０）が指定したＩＰアドレスＡ（Ｕｎ）のピアツーピア型匿名プロキシのＰ（Ｕｎ）を通っていない、もしくはＰ（Ｕｎ）かチェック用匿名通信路上にあるピアツーピア型匿名プロキシが正しく動作していないと判断できる。そのため、現在構築中の匿名通信路は信頼できないものとし、図６のステップＳ１へ飛び、今回使われたＩＰアドレス以外のピアツーピア型匿名プロキシを用いて、新たに匿名通信路の確保を行うようにする。Ｐ（Ｕ０）とＰ（Ｕｎ）間で送受信したデータがパスワードＰＷ（Ｕｎ）で一致する場合（ステップＳ２０）には、図６のステップＳ２１へ飛ぶ。

【００５１】

Ｐ（Ｕ０）は、変数ｍとｎが一致するか確認する（ステップＳ２１）。一致する場合に

は、データ送受信用匿名通信路上にあるピアツーピア型匿名プロキシを全てチェックし終えたことになり、図６のステップＳ２３へ飛ぶ。逆に変数ｍとｎが一致しない場合（ステップＳ２１）には、データ送受信用匿名通信路上のピアツーピア型匿名プロキシ全てをチェックしていないことになり、Ｐ（Ｕ０）は変数ｎに１を加算し（ステップＳ２２）、図６のステップＳ１９へ飛びチェックを続ける。

【００５２】

Ｐ（Ｕ０）において、ユーザＵ０から終了命令があるか確認する（ステップＳ２３）。終了命令がある場合には、匿名通信路の確保を中断し終了する。終了命令が無い場合には、ユーザＵ０からｗｅｂブラウザなどでＰ（Ｕ０）に対してアクセスがあるか確認する（ステップＳ２４）。ある場合には、図６のステップＳ２６へ飛び、無い場合には図６のステップＳ２５へ飛ぶ。そこで、ユーザＵ０から経路変更の命令があるか確認する（ステップＳ２５）。経路変更の命令がある場合には、図６のステップＳ１に飛び、データ送受信用匿名通信路を再度確保する。経路変更の命令が無い場合には、図６のステップＳ２３へ飛び、処理を繰り返す。

【００５３】

ユーザＵ０はｗｅｂブラウザから、自分が立ち上げているピアツーピア型匿名プロキシのＰ（Ｕ０）へ接続する。そして、Ｕ０のｗｅｂブラウザから Ｐ（Ｕ０）へ暗号化せず、アクセスしたいＵＲＬなどを送る（ステップＳ２６）。この場合、Ｕ０が操作しているパソコンとピアツーピア型匿名プロキシが存在するコンピュータは同一、もしくは同じノードのネットワーク上にあるため、暗号化しなくてもその内容を秘匿できる。同一ノードにない場合や、同じノードのネットワーク上でも暗号化を行いたい場合はこの限りでない。その後、Ｐ（Ｕ０）からＰ（Ｕｍ）へ公開鍵ＬＰ１（Ｕｍ）で暗号化し、ユーザＵ０から受け取ったＵＲＬを送る。Ｐ（Ｕｍ）は受け取ったデータを秘密鍵ＬＳ１（Ｕｍ）で復号化する（ステップＳ２７）。このとき、Ｐ（Ｕ０）からＰ（ｍ）へは直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｕ０）からＰ（Ｕ１）へ、Ｐ（Ｕ１）からＰ（Ｕ２）へ、という順でＰ（Ｕｍ）へ送る（図７）。

【００５４】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｕ０）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図６のステップＳ２７の公開鍵ＬＰ１（Ｕｍ）で暗号化したユーザＵ０のリクエストＵＲＬに相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｕｍ）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｕｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｕｋ＋１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｕｋ＋１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｕｍ）が一致する場合（ステップＳ３４）、図６のステップＳ２８に飛ぶ。

【００５５】

ＵＲＬを受け取ったＰ（Ｕｍ）は、そのＵＲＬのｗｅｂサーバＳＶへアクセスする（ステップＳ２８）。そして、サーバＳＶからデータｈｔｍｌを受け取る（ステップＳ２９）。この通信は暗号化されていないが、Ｗｅｂサーバ自体がＳＳＬなどで暗号化されている場合はこの限りでない。

【００５６】

Ｐ（Ｕｍ）からＰ（Ｕ０）へ公開鍵ＬＰ２（Ｕ０）で暗号化し、ＳＶから受け取ったデータｈｔｍｌを送る。Ｐ（Ｕ０）は受け取ったデータを秘密鍵ＬＳ２（Ｕ０）で復号化する（ステップＳ３０）。このとき、Ｐ（Ｕｍ）からＰ（Ｕ０）へは直接送らずに、隣り合わせでつながっている中継点同士暗号通信を行いながら、Ｐ（Ｕｍ）からＰ（Ｕｍ－１）へ、Ｐ（Ｕｍ－１）からＰ（Ｕｍ－２）へ、という順でＰ（Ｕ０）へ送る（図７）。

【００５７】

図７のフローチャートにおいて、Ｐ（Ｒ０）はＰ（Ｕｍ）と同一のピアツーピア型匿名プロキシである。ＤＡＴＡ（Ｒ０）は、図６のステップＳ３０の公開鍵ＬＰ２（Ｕ０）で暗号化したＳＶからのデータｈｔｍｌに相当する（ステップＳ３２）。変数ｋはフローチャートを説明するための便宜上のもの（ステップＳ３３）であり、どのピアツーピア型匿名プロキシにもこの変数は存在しない。Ｐ（Ｒｋ）とＰ（Ｕ０）が一致しない場合（ステップＳ３４）、Ｐ（Ｒｋ）からＰ（Ｒｋ＋１）へ公開鍵ＬＰ１（Ｒｋ＋１）で暗号化し、ＤＡＴＡ（Ｒ０）を送る（ステップＳ３５）。ここでは、Ｐ（Ｒｋ）はＰ（Ｕｍ－ｋ）に、Ｐ（Ｒｋ＋１）はＰ（Ｕｍ－ｋ－１）に、公開鍵ＬＰ１（Ｒｋ＋１）は公開鍵ＬＰ１（Ｕｍ－ｋ－１）に相当する。その後、変数ｋに１を加算し、図７のステップＳ３４へ飛ぶ（ステップＳ３６）。Ｐ（Ｒｋ）とＰ（Ｕ０）が一致する場合（ステップＳ３４）、図６のステップＳ３１に飛ぶ。

【００５８】

データを受け取ったＰ（Ｕ０）からユーザＵ０が使用しているｗｅｂブラウザへ暗号化せず、データｈｔｍｌを送る（ステップＳ３１）。この場合、Ｕ０が操作しているパソコンとピアツーピア型匿名プロキシが存在するコンピュータは同一、もしくは同じノードのネットワーク上にあるため、暗号化しなくてもその内容を秘匿できる。同一ノードにない場合や、同じノードのネットワーク上でも暗号化を行いたい場合はその限りでない。このｗｅｂサーバＳＶとのデータ送受信を必要な分だけ、図６のステップＳ２３からＳ３１まで繰り返す。

【００５９】

これらの図６における手順のユーザＵ０からサーバＳＶまでの匿名通信路のデータ決定、生成、送受信を表したものが図９である。コンピュータの項目には、データ送受信におけるユーザＵ０やピアツーピア型匿名プロキシ、サーバＳＶが記載されている。該当ステップでは、図６のフローチャートにおけるステップを示している。表の上から下に時間が経過する。なお、図６と図８のフローチャートはほぼ同しデータの流れとなるため、図８に対応した匿名通信路のデータ決定、生成、送受信図は省略する。

【００６０】

また、図７におけるピアツーピア型匿名プロキシ間のデータ送受信を説明したものが図１０である。コンピュータの項目には、ピアツーピア型匿名プロキシが記載されており、データはＰ（Ｒ０）からＰ（Ｒｈ）へ送信する場合の流れが記載されている。該当ステップでは、図７のフローチャートにおける手順を示している。表の上から下に時間が経過する。

【産業上の利用可能性】

【００６１】

この手法を用いることにより、インターネットサービスプロバイダや特定の団体が用意する匿名プロキシを使用することなく、インターネットを利用する個人個人がプライバシーを保護するプログラムを立ち上げることが可能になる。

【００６２】

現在ではプロバイダの管理により、国内における個人のアクセス情報は厳重管理されている。これは、特定の条件を満たさない限り、第三者が見ることはできない。しかし、現実にはプロバイダ側の管理ミスや、内外部からのハッキングによりこれらの個人情報が流出する危険性がある。

【００６３】

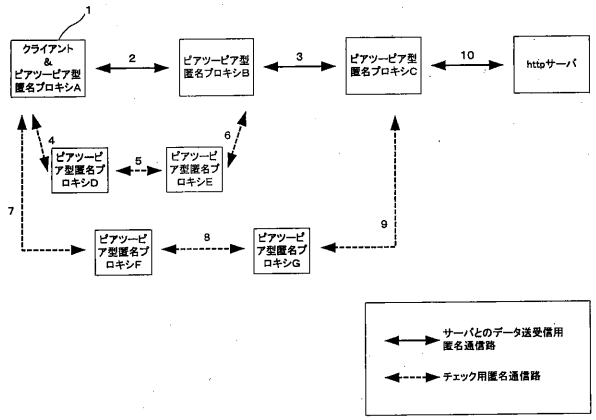
これらの危険性を自ら守ることができるため、より手軽にプライバシーや秘密の保護が行えるようになる。使用者のインターネットにおけるデータ漏洩に対する不安を取り除き、インターネットの使用の活性化を促進させるものとなる。

【００６４】

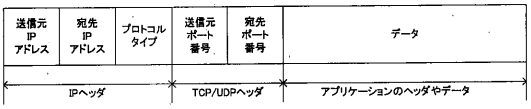
また、このシステムを利用することにより、インターネットを使用した内部告発などにおいて、告発者の身元を安全に保護することが可能になる。そのため、社会や企業内部で行われている違法行為の告発を促進し、健全な社会及び経済形成を構築することに一役買

うことが可能となる。
【図面の簡単な説明】
【００６５】
【図１】匿名通信路確定手順図である。（発明を実施するための最良の形態）
【図２】ＩＰパケット構成の概念図である。（背景技術）
【図３】インターネット上の接続概念図である。（背景技術）
【図４】匿名プロキシを経由した接続の概念図である。（背景技術）
【図５】ピアツーピア型匿名プロキシの匿名通信の概念図である。（背景技術）
【図６】ピアツーピア型匿名プロキシ間の動作フローチャートである。（実施例）
【図７】ピアツーピア型匿名プロキシ間の動作フローチャートである。（実施例）
【図８】ピアツーピア型匿名プロキシ間の動作フローチャートである。（実施例）
【図９】図６におけるピアツーピア型匿名プロキシ間のデータ決定、生成、送受信図である。（実施例）
【図１０】図７におけるピアツーピア型匿名プロキシ間のデータ決定、生成、送受信図である。（実施例）
【符号の説明】
【００６６】
１　クライアント及び、ピアツーピア型匿名プロキシを立ち上げているコンピュータ
２　ピアツーピア型匿名プロキシＡとピアツーピア型匿名プロキシＢの接続
３　ピアツーピア型匿名プロキシＢとピアツーピア型匿名プロキシＣの接続
４　ピアツーピア型匿名プロキシＡとピアツーピア型匿名プロキシＤの接続
５　ピアツーピア型匿名プロキシＤとピアツーピア型匿名プロキシＥの接続
６　ピアツーピア型匿名プロキシＥとピアツーピア型匿名プロキシＢの接続
７　ピアツーピア型匿名プロキシＡとピアツーピア型匿名プロキシＦの接続
８　ピアツーピア型匿名プロキシＦとピアツーピア型匿名プロキシＧの接続
９　ピアツーピア型匿名プロキシＧとピアツーピア型匿名プロキシＣの接続
１０　ピアツーピア型匿名プロキシＣとｈｔｔｐサーバの接続
２０　クライアントとｈｔｔｐサーバの接続
２１　匿名プロキシＡ
２２　匿名プロキシＣとｈｔｔｐサーバの接続

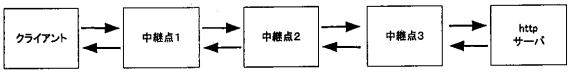
【図１】



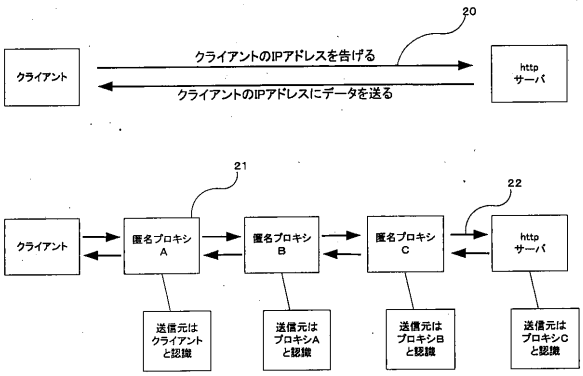
【図２】



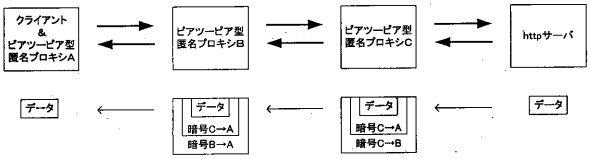
【図３】



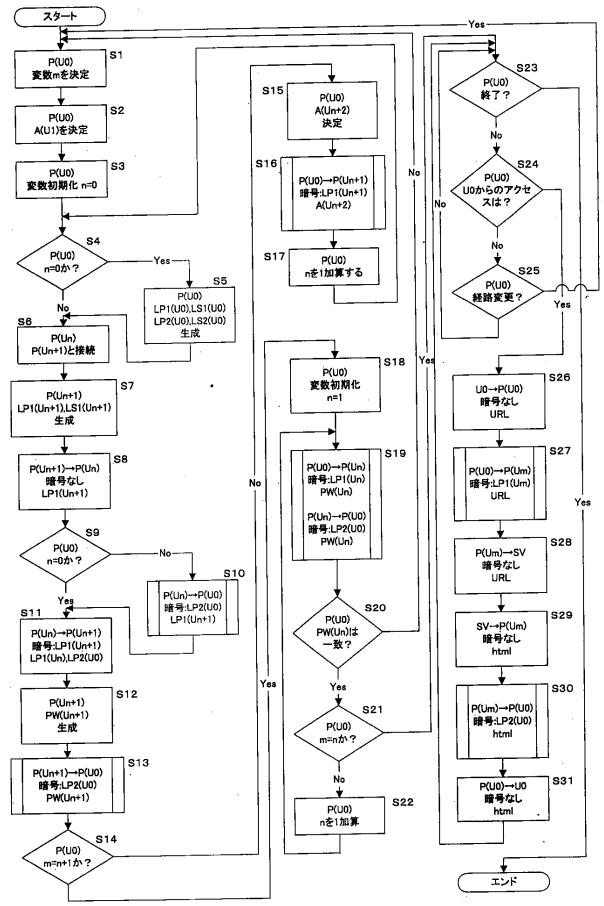
【図４】



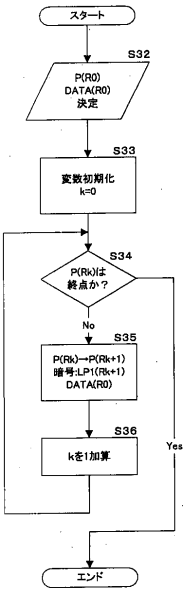
【図５】



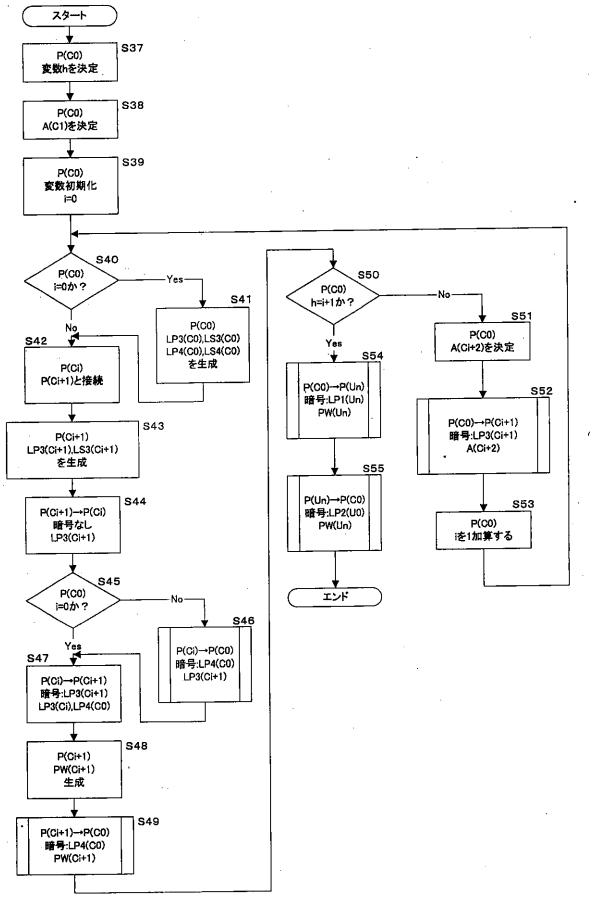
【図６】



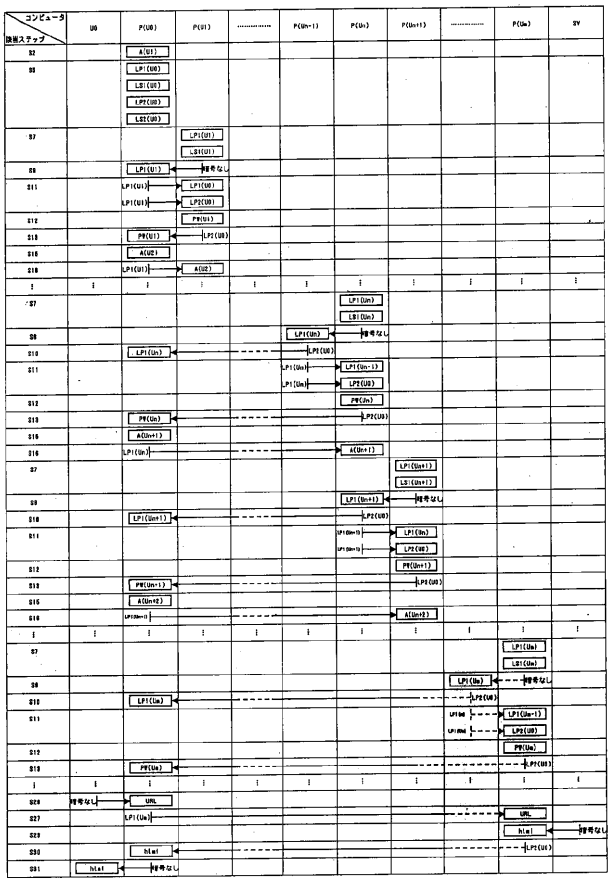
【図７】



【図８】



【図９】



【図１０】

コンピュータ / 該当ステップ	P(R0)	P(R1)	……	P(Rk-1)	P(Rk)	P(Rk+1)	……	P(Rh)
S92	DATA(R0)							
S93	LP1(R1)	DATA(R0)						
S94		LP1(R2)	DATA(R0)					
S95			LP1(Rk-1)	DATA(R0)				
S96				LP1(Rk)	DATA(R0)			
S95					LP1(Rk+1)	DATA(R0)		
S95						LP1(Rk+2)	DATA(R0)	
S96							LP1(Rh)	DATA(R0)

フロントページの続き

Ｆターム(参考) 5B285 AA04 BA01 CA04 CA43 CB02 CB52 CB76 DA05
5J104 AA07 AA16 EA03 EA15 EA16 KA02 KA04 NA05 NA27 NA38
PA07
5K030 GA15 HA08 HD03 JA11 KA05 LB02 LB05 LD19