

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2010 年 9 月 10 日(10.09.2010)

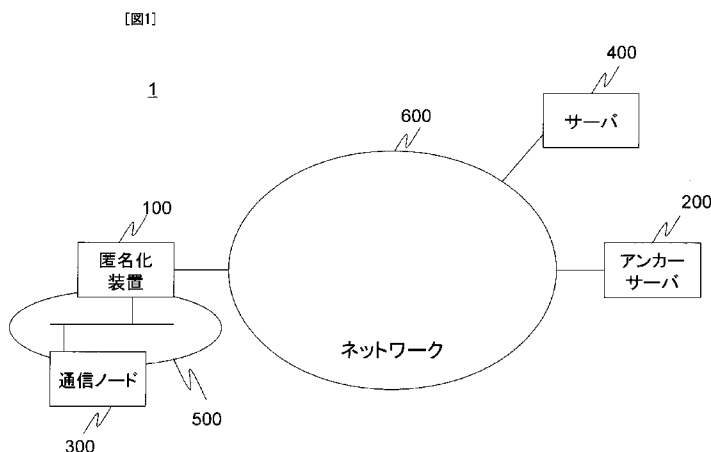
PCT

(10) 国際公開番号
WO 2010/100850 A1

- (51) 国際特許分類:
H04L 12/46 (2006.01) H04L 12/66 (2006.01)
H04L 12/56 (2006.01)
- (21) 国際出願番号: PCT/JP2010/001110
- (22) 国際出願日: 2010 年 2 月 19 日(19.02.2010)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2009-052919 2009 年 3 月 6 日(06.03.2009) JP
- (71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC Corporation) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号 Tokyo (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 栗野潤 (AWANO, Jun) [JP/JP]; 〒1088001 東京都港区芝五丁目 7 番 1 号日本電気株式会社内 Tokyo (JP).
- (74) 代理人: 家入健 (IEIRI, Takeshi); 〒2210835 神奈川県横浜市神奈川区鶴屋町三丁目 3 3 番 8 アサヒビルディング 10 階響国際特許事務所 Kana-gawa (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告 (条約第 21 条(3))

(54) Title: COMMUNICATION METHOD, COMMUNICATION SYSTEM, ANONYMIZING DEVICE, AND SERVER

(54) 発明の名称: 通信方法、通信システム、匿名化装置、サーバ



100 anonymizing device
300 communication node
600 network
400 server
200 anchor server

(57) Abstract: A communication system (1) comprising an anonymizing device(100) and a server (200). The anonymizing device (100) generates an anonymous address based on a prefix obtained from the server (200); rewrites the source address of a packet, when one transmitted from a communication node (300) has been received, to an anonymous address; then, after encapsulating the received packet, sends the packet to a second network (600) using the address of the anonymizing device (100) as the source address of the encapsulated packet and the address of the server (200) as the destination address. Then, when the server (200) has received the encapsulated packet transmitted from the anonymizing device (100), the server (200) de-encapsulates the encapsulated packet and transfers the packet to the second network (600). Due to this, high anonymity can be secured.

(57) 要約: 本発明に係る通信システム (1) は、匿名化装置 (100) とサーバ (200) とを有する。匿名化装置 (100) は、サーバ (200) から取得したプレフィクスに基づいて、匿名アドレスを生成し、通信ノード (300) から送信されたパケットを受信した場合

に、受信パケットの送信元アドレスを匿名アドレスに書き換え、受信パケットをカプセル化した後に、カプセル化パケットの送信元アドレスを匿名化装置 (100) のアドレスとし、かつ、送信先アドレスをサーバ (200) のアドレスとして第2のネットワーク (600) に送出する。そして、サーバ (200) は、匿名化装置 (100) から送信されたカプセル化パケットを受信した場合に、カプセル化パケットをデカプセル化して第2のネットワーク (600) に送出する。これにより、高い匿名性を確保することができる。

WO 2010/100850 A1

明 細 書

発明の名称：通信方法、通信システム、匿名化装置、サーバ 技術分野

[0001] 本発明は、IP（Internet Protocol）を使用して通信を行う通信方法、通信システム、匿名化装置、サーバに関し、特にIPv6（Internet Protocol Version 6）に基づいてネットワーク全体の中で一意となるアドレスを使用して通信を行う場合においても、通信ノードの匿名性を確保可能な通信方法、通信システム、匿名化装置、サーバに関する。

背景技術

[0002] 近年、IPv4のアドレスの枯渇が現実を帯びてきており、IPv6への移行が本格的に始まろうとしている。IPv4のアドレス空間が32bitであったのに対して、IPv6のアドレス空間は128bitもの広大なアドレス空間を有している。このため、IPv6では、グローバルな範囲でユニークなIPv6アドレスを全てのノードに割当てることができる。IPv4のように、NAT（Network Address Translation）を使用して、1つのパブリックなIPv4アドレスを複数のノードで共用する必要がない。従って、IPv6では、個々のノードは、エンド・トゥー・エンド通信を実現することができる。これは、インターネットの当初の設計思想に適うものであり、大きなメリットがある。例えば、NATを超えるために様々な工夫を強いられたP2P系のアプリケーションを、より容易に実現することができるメリットがある。

[0003] 一方で問題もある。IPv6を使用した通信においては、上述のように各ノードにして割当てられたアドレスが通信相手に知られることになる。しかも、IPv6の自動アドレス設定機能を用いて生成されたIPv6アドレスは、その下位64bitがNIC（Network Interface Card）のMAC（Media Access Control）アドレスに使用される。さらに、MACアドレスに使用されるIPv6アドレスの下位64bitは、長期的、かつ、固定的に用い

られる。この結果、通信ノードの使用ユーザの通信履歴が追跡される危険性が大きく、匿名性確保の面で大きな問題がある。

[0004] また、NATを使用した通信においては、通信を行うノード自身のアドレスは、通信相手に対して隠蔽される。例えば、ノードからWEBサーバへのアクセスが行われた場合には、WEBサーバは、WAN（Wide Area Network）側に割当てられたNATのアドレスを知ることができるが、NAT配下のLAN（Local Area Network）のアドレスについては知ることができない。多くの場合、各ホームに配布されたブロードバンドルータに、WAN側のアドレスが割当てられる。このため、WAN側のアドレスを知ること、その時点での通信元となるホームを特定することは可能であるが、WAN側のアドレスは一時的なものであり、NATが実装されたブロードバンドルータの再起動時など、様々な契機に変化する。従って、特定のノードの通信を、長期に渡って追跡することはできない。

[0005] ところで、匿名性確保の問題を解決するため、IPv6アドレスの下位64bitについて、MACアドレスを使用せずにランダムに生成するものとし、さらに、これを定期的に変更する仕様が公開されている（非特許文献1：RFC3041, 「Privacy Extensions for Stateless Address Autoconfiguration in IPv6」）。

[0006] しかし、非特許文献1に開示される仕様に基づく手法においても、IPv6の上位64bit部分であるプレフィクス部については、変更されないままである。ここで、IPv6の上位64bitを示すプレフィクスは、例えば、ホームに配布されたブロードバンドルータに割当てられ、ブロードバンドルータの配下のLANに接続した通信ノードに広告される。この結果、通信ノードは、受信したプレフィクスを上位64bitに配置したIPv6アドレスを生成し、その生成したIPv6アドレスを使用して通信を行う。

[0007] IPv6のプレフィクス部が長期間に渡って変更されない場合には、ホーム単位で通信元が特定される危険がある。このような危険があるケースは、現在のIPv4でNATを使用したケースと類似するが、上述したように、

I P v 4 では、N A T の W A N 側のアドレスは様々な契機に変更される。

[0008] I P v 6 の場合には、プレフィクスを使用することで、L A N に接続した通信ノードのアドレスを生成するため、プレフィクスの変更は、L A N 内の通信ノードのアドレスの変更を伴う。このため、I P v 4 における N A T の W A N 側のアドレスのように、プレフィクスが定期的に変更されることは問題となる。結果として、I P v 6 では固定的なプレフィクスを長期的に使用することになり、I P v 4 の場合と比較して、匿名性の問題はより大きいといえる。

[0009] さらに、I P v 6 では、P 2 P 系のアプリケーションが今後も増加していくものと考えられ、また、各ユーザが使用する通信ノードのアドレスをユーザ同士で直接的に知る機会が多くなることから、匿名性の問題がより重大なものになると考えられる。従って、I P v 6 では、I P v 4 と比較して、より高い匿名性が必要になる。

[0010] また、L A N 内の通信ノードが、プレフィクス部も含めて自らのアドレスを勝手に変更してしまうことにも問題がある。その理由は、プレフィクス部は I P v 6 パケットのルーティングに用いられるため、プレフィクス部を変更した場合には、通信ノード宛のパケットを、通信ノードが接続するネットワークまでルーティングできなくなるためである。

[0011] プレフィクス部も含めたアドレス変更を実現する方式の一例が、特許文献 1 に開示されている。以下、特許文献 1 に係る通信システムにおける動作を簡単に説明する。図 2 7 に示すように、特許文献 1 に係る通信システムは、発信側情報処理装置 p 1 0 (アドレス=2・7 F F F F 0・6 E 9 A) と、仮アドレスサーバ p 2 0 (アドレス=5・5 F F F F 0・0 0 0) と、受信側情報処理装置 p 3 0 (アドレス=2・7 F F F F 0・6 3 9 A) と、から構成され、インターネット p 4 0 を介してそれぞれ接続されている。

[0012] 発信側情報処理装置 p 1 0 は、パケットを送信する際に、仮アドレスサーバ p 2 0 から仮アドレス (5・5 F F F F 0・0 0 0 1) を取得し、取得した仮アドレスをパケットの送信時の送信元アドレスとして使用する。すなわ

ち、発信情報処理装置 p 1 0 は、送信パケット（ $d s t = 2 \cdot 7 F F F F 0 \cdot 6 3 9 A$ 、 $s r t = 5 \cdot 5 F F F F 0 \cdot 0 0 0 1$ （仮アドレス））を受信側情報処理装置 p 3 0 に送信する。

[0013] 受信側情報処理装置 p 3 0 は、発信側情報処理装置 p 1 0 から送信されたパケットを受信すると、その応答を送信元アドレス（ $5 \cdot 5 F F F F 0 \cdot 0 0 0 1$ ）に応答する。このアドレスは、仮アドレスサーバ p 2 0 にルーティングされるプレフィクス部を有するアドレスとなっているため、仮アドレスサーバ p 2 0 が応答パケットを受信する。すなわち、仮アドレスサーバ p 2 0 は、受信側情報処理装置 p 3 0 から、受信パケット（ $d s t = 5 \cdot 5 F F F F 0 \cdot 0 0 0 1$ （仮アドレス）、 $s r c = 2 \cdot 7 F F F F 0 \cdot 6 3 9 A$ ）を受信する。

[0014] 仮アドレスサーバ p 2 0 は、発信側情報処理装置 p 1 0 に仮アドレスを割当てる際に、発信側情報処理装置 p 1 0 の実アドレス（ $2 \cdot 7 F F F F 0 \cdot 6 E 9 A$ ）と貸し出した仮アドレス（ $5 \cdot 5 F F F F 0 \cdot 0 0 0 1$ ）との対応関係を保持しておき、この保持した情報を使用することで、受信側情報処理装置 p 3 0 から送信されたパケットが発信側情報処理装置 p 1 0 へと送信すべきパケットであったことを知る。この結果、仮アドレスサーバ p 2 0 は、受信側情報処理装置 p 3 0 から受信したパケットについて、宛先アドレスを発信側情報処理装置 p 1 0 の実アドレスに、送信元アドレスを仮アドレスサーバ p 2 0 のアドレス（ $5 \cdot 5 F F F F 0 \cdot 0 0 0 0$ ）にそれぞれ変更して、インターネット p 4 0 に送出する。

[0015] 最終的に、仮アドレスサーバ p 2 0 から送信されたパケットが発信側情報処理装置 p 1 0 にルーティングされ、発信側情報処理装置 p 1 0 がこれを受信する。以上説明した方法によれば、発信側情報処理装置 p 1 0 は、プレフィクス部も含めてアドレスを変更することができる。すなわち、発信側情報処理装置 p 1 0 は、仮アドレスサーバ p 2 0 から、受信パケット（ $d s t = 2 \cdot 7 F F F F 0 \cdot 6 E 9 A$ 、 $s r c = 5 \cdot 5 F F F F 0 \cdot 0 0 0 0$ （仮アドレスサーバ））を受信する。

- [0016] また、他の関連する技術として、特許文献2には、Mobile IPv6において、匿名アドレスを作成する機能や、トンネル機能を有するトンネルサーバを備えたサーバ装置が開示されている。特許文献3には、IPv6ネットワークアクセス網において、IF-IDとIPv6アドレスPrefixとを組み合わせ、グローバルIPv6アドレスを設定するユーザ管理方法が開示されている。特許文献4には、ハッシュ関数のダイジェスト値に基づいて端末のインタフェースIDを算出し、算出した端末のインタフェースIDを用いて送信元アドレスを生成する通信装置が開示されている。

先行技術文献

特許文献

- [0017] 特許文献1：特開2007-189752号公報
特許文献2：特開2003-298657号公報
特許文献3：特開2004-242142号公報
特許文献4：特開2005-079921号公報

非特許文献

- [0018] 非特許文献1：RFC3041「Privacy Extensions for Stateless Address Autoconfiguration in IPv6」

発明の概要

発明が解決しようとする課題

- [0019] しかしながら、特許文献1に係る通信システムには、以下に説明する問題がある。

(問題1)

発信側情報処理装置p10がパケットを送信する際の送信元アドレスは、発信側情報処理装置p10が接続したネットワークのプレフィクスとは異なるものとなる。発信側情報処理装置p10とインターネットp40との境界に配置されるルータでは、セキュリティの観点から、発信側情報処理装置p10が送信するこのようなパケットを破棄する場合があります（このフィルタリ

ング処理をイングレスフィルタという)、このような場合には、発信側情報処理装置 p 1 0 は通信することができない。

[0020] (問題 2)

上述したように、発信側情報処理装置 p 1 0 が送信するパケットの送信元アドレス及び宛先アドレスと、受信側情報処理装置 p 3 0 が応答するパケットの宛先アドレス及び送信アドレスと、は異なるアドレスとなる。TCP (Transmission Control Protocol) などのコネクションを確立するプロトコルでは、両端点 (発信側情報処理装置 p 1 0 及び受信側情報処理装置 p 3 0) のアドレス及びポートのペアを用いてコネクションを確立する。従って、特許文献 1 に係る通信システムでは、送受信時のパケットの両端点のアドレスが一致しないため、TCP を用いた通信ができない。TCP は、HTTP (Hypertext Transfer Protocol) や FTP (File Transfer Protocol) などの、多数の上位プロトコルが利用している。このため、TCP を用いた通信ができないことは、それら多数の上位プロトコルを使用できないことを意味する。

[0021] (問題 3)

特許文献 1 に係る通信システムでは、発信側情報処理装置 p 1 0 が、仮アドレスを取得及び返却する機能や、送信パケットの送信元アドレスとして使用するアドレスを選択する機能といった特殊な機能を備えている必要がある。現在、IPv6 機能を備えた装置の普及が既に始まっている。装置として、例えば、Windows Vista (登録商標) を搭載した PC (Personal Computer) が該当する。この様な状況において、通信ノード側に特殊な機能を要する方式の適用は非常に難しい。また、特定のアプリケーションを使用して対応することは可能であるが、WEB ブラウザなどのように、高頻度で使用する従来のアプリケーションに適用可能でなければ、匿名性を確保する意義が希薄となる。

[0022] (問題 4)

仮に、特許文献 1 に係る通信システムを適用した WEB ブラウザが存在す

る場合においても、昨今のWEBサービスでは、複数の通信を同時に並列して行うものがある。このようなWEBサービスでは、発信側情報処理装置p10に複数のIPv6仮アドレスが付与されることとなる。この場合に、発信側情報処理装置p10は、新たなアドレスを取得する度に、アドレス重複検出手順であるDAD (Duplicate Address Detection) を実施する必要があるため、負荷や通信のレスポンス、ネットワーク帯域の利用効率などの面で問題となる。さらには、同じネットワークに接続する他の通信ノードにおいても、発信側情報処理装置p10に付与される複数のアドレスの情報をキャッシュに保持する必要があるため、負荷が大きくなる。

[0023] 本発明は、上述した問題を鑑みなされたものであり、その目的は、通信ノード自体に対する変更を必要とすることなく、従来のアプリケーションを使用した通信に対して、高い匿名性を確保することが可能な通信方法、通信システム、匿名化装置、サーバを提供することである。

課題を解決するための手段

[0024] 本発明に係る第1の態様の通信システムは、通信ノードと第1のネットワークを介して接続される匿名化装置と、当該匿名化装置と第2のネットワークを介して接続されるサーバと、を有する通信システムであって、前記匿名化装置は、前記サーバから取得したプレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットの送信元アドレスを前記匿名アドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備え、前記サーバは、前記匿名化装置から送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第2のネットワークに送出する転送手段を備えるものである。

[0025] 本発明に係る第2の態様の通信システムは、通信ノードと第1のネットワ

ークを介して接続される匿名化装置と、当該匿名化装置と第2のネットワークを介して接続されるサーバと、を有する通信システムであって、前記匿名化装置は、前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備え、前記サーバは、プレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、前記匿名化装置から送信されたカプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信元アドレスを前記匿名アドレスに書き換えた後に、当該デカプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備えるものである。

[0026] 本発明に係る第3の態様の通信方法は、通信ノードと第1のネットワークを介して接続される匿名化装置と、当該匿名化装置と第2のネットワークを介して接続されるサーバと、を有する通信システムにおける通信方法であって、前記匿名化装置は、前記通信ノードから送信されたパケットを受信した場合に、前記サーバから取得したプレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成ステップと、当該受信パケットの送信元アドレスを前記匿名アドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理ステップと、を有し、前記サーバは、前記匿名化装置から送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第2のネットワークに送出する転送ステップを有することを特徴とするものである。

[0027] 本発明に係る第4の態様の通信方法は、通信ノードと第1のネットワークを介して接続される匿名化装置と、当該匿名化装置と第2のネットワークを

介して接続されるサーバと、を有する通信システムにおける通信方法であって、前記匿名化装置は、前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理ステップと、を有し、前記サーバは、前記匿名化装置から送信されたカプセル化パケットを受信した場合に、プレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成ステップと、当該カプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信元アドレスを前記匿名アドレスに書き換えた後に、当該デカプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとして前記第2のネットワークに送出するパケット処理ステップと、を有するものである。

[0028] 本発明に係る第5の態様の匿名化装置は、第1のネットワークを介して接続される通信ノードから送信されたパケットを受信した場合に、第2のネットワークを介して接続されるサーバから取得したプレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、前記通信ノードからの送信されたパケットの送信元アドレスを前記匿名アドレスに書き換え、当該パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを自身のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備えるものである。

[0029] 本発明に係る第6の態様のサーバは、匿名化装置と第1のネットワークを介して接続される通信ノードから送信されたパケットであって、かつ、前記匿名化装置によりカプセル化された後に第2のネットワークを介して送信されたパケットを受信した場合に、プレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、前記匿名化装置から送信されたカプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信元アドレスを前記匿名アドレスに書き換えた後に、当該デカプセル化パケットの送信元

アドレスを前記匿名化装置のアドレスとして前記第 2 のネットワークに送出するパケット処理手段と、を備えるものである。

[0030] 本発明に係る第 7 の態様の通信システムは、通信ノードと第 1 のネットワークを介して接続される匿名化装置と、当該匿名化装置と第 2 のネットワークを介して接続されるサーバと、を有し、前記匿名化装置は、前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットの送信元アドレスを前記サーバから取得した匿名アドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第 2 のネットワークに送出するパケット処理手段を備え、前記サーバは、前記匿名化装置から送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第 2 のネットワークに送出する転送手段を備えるものである。

[0031] 本発明に係る第 8 の態様の匿名化装置は、第 1 のネットワークを介して接続される通信ノードから送信されたパケットを受信した場合に、第 2 のネットワークを介して接続されるサーバから匿名アドレスを取得し、前記通信ノードからの送信されたパケットの送信元アドレスを前記取得した匿名アドレスに書き換え、当該パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを自身のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第 2 のネットワークに送出するパケット処理手段を備えるものである。

発明の効果

[0032] 本発明によれば、高い匿名性を確保することが可能な通信システム、通信方法、匿名化装置、サーバを提供することができる。

図面の簡単な説明

[0033] [図1] 本発明の実施の形態 1 に係る通信システムの全体構成を示す図である。

[図2] 本発明の実施の形態 1 に係る匿名化装置の構成を示す図である。

[図3] 本発明の実施の形態 1 に係る匿名化ポリシーテーブルを示す図である。

[図4]本発明の実施の形態1に係るセッション管理テーブルを示す図である。

[図5]本発明の実施の形態1に係るプレフィクス情報テーブルを示す図である。

。

[図6]本発明の実施の形態1に係るアンカーサーバの構成を示す図である。

[図7]本発明の実施の形態1に係る貸出しプレフィクステーブルを示す図である。

[図8]本発明の実施の形態1に係る転送テーブルを示す図である。

[図9]本発明の実施の形態1に係る匿名化装置の動作を示すフローチャートである。

[図10]本発明の実施の形態1に係る匿名化装置のプレフィクス決定処理を示すフローチャートである。

[図11]本発明の実施の形態1に係る匿名化装置のプレフィクス要求処理を示すフローチャートである。

[図12]本発明の実施の形態1に係る匿名化装置のパケット処理を示すフローチャートである。

[図13]本発明の実施の形態1に係るアンカーサーバでのプレフィクス割当要求を受信した際の動作を示すフローチャートである。

[図14]本発明の実施の形態1に係るアンカーサーバでのパケット転送処理の動作を示すフローチャートである。

[図15]本発明の実施の形態1に係る匿名化装置とアンカーサーバの動作を示すシーケンス図である。

[図16]新たなエントリが追加されたプレフィクス情報テーブルの例を示す図である。

[図17]新たなエントリが追加されたセッション管理テーブルの例を示す図である。

[図18]新たなエントリが追加された転送テーブルの例を示す図である。

[図19]本発明の実施の形態2に係る匿名化装置の構成を示す図である。

[図20]本発明の実施の形態2に係るアンカーサーバの構成を示す図である。

[図21]本発明の実施の形態2に係る匿名化装置が保持するセッション管理テーブルを示す図である。

[図22]本発明の実施の形態2に係るアンカーサーバが保持するセッション管理テーブルを示す図である。

[図23]本発明の実施の形態2に係るアンカーサーバが保持するプレフィクス情報テーブルである。

[図24]本発明の実施の形態2に係る匿名化装置の動作を示すフローチャートである。

[図25]本発明の実施の形態2に係るアンカーサーバの構成を示す図である。

[図26]本発明の実施の形態2に係るアンカーサーバでのパケット転送処理の動作を示すフローチャートである。

[図27]関連する通信システムの構成を示す図である。

発明を実施するための形態

[0034] 実施の形態1.

以下、図面を参照して本発明の実施の形態1について説明する。

(構成の説明)

まず、図1乃至図8を参照して、本実施の形態1に係る通信システム1の構成について説明する。図1は、本実施の形態1に係る通信システム1を示す全体構成図である。通信システム1は、匿名化装置100と、アンカーサーバ200と、通信ノード300と、サーバ400と、を備えている。通信ノード300は、ローカルネットワーク500を介して匿名化装置100に接続される。また、匿名化装置100と、アンカーサーバ200と、サーバ400と、はネットワーク600を介してそれぞれ接続される。

[0035] 匿名化装置100は、(A)受信したパケットのセッションを識別する機能と、(B)セッション単位で、パケットの送信元アドレスを、アンカーサーバ200から取得したプレフィクス群から1つ選択して生成したアドレスに書き換える機能と、(C)書き換えたアドレスを用いて到達できるアンカーサーバ200に、パケットをトンネリングする機能と、を備えている。尚

、以下では、通信ノード２００が実施する通信に関して、通信の一連のまとまりである単位をセッションと称する。

[0036] 図２は、匿名化装置１００を示す構成図である。図に示すように、匿名化装置１００は、インタフェース１１０Ａと、インタフェース１１０Ｂと、匿名化制御手段１２０と、パケット処理手段１３０と、情報記録装置１４０と、を備えている。

[0037] インタフェース１１０Ａは、ローカルネットワーク５００に接続され、ローカルネットワーク５００に接続した他のノード（通信ノード３００など）との間でパケットの送受信を行うためのインタフェースである。インタフェース１１０Ａから入力されたパケットは、匿名化制御手段１２０に出力される。また、パケット処理手段１３０がローカルネットワーク５００に接続したノード宛に送信したパケットは、インタフェース１１０Ａを介してローカルネットワーク５００に送出される。

[0038] インタフェース１１０Ｂは、ネットワーク６００に接続され、ネットワーク６００に接続した他のノード（アンカーサーバ２００など）との間でパケットの送受信を行うためのインタフェースである。インタフェース１１０Ｂから入力されたパケットは、パケット処理手段１３０に出力される。また、パケット処理手段１３０がネットワーク６００に接続したノードに送信したパケットは、インタフェース１１０Ｂを介してネットワーク６００に送出される。

[0039] 匿名化制御手段１２０は、匿名性確保要否判定手段１２１と、セッション管理手段１２２と、匿名アドレス選択手段１２３と、匿名アドレス生成手段１２４と、を備えている。

[0040] 匿名性確保要否判定手段１２１は、インタフェース１１０Ａから入力されたパケットの情報を読み取り、読み取った情報に基づいて、入力されたパケットに対して匿名性を確保する必要があるか否かを判定する機能を備えている。尚、本実施の形態１においては、入力されたパケットの情報として、送信元アドレスと、宛先アドレスと、送信元ポート番号と、宛先ポート番号と

、プロトコル種別と、を用いて説明するが、他の情報を用いるものとしても良い。

[0041] 匿名性確保要否判定手段 121 は、匿名性の要否を判定する場合に、（A）情報記録装置 140 に記録された匿名化ポリシーテーブルにアクセスする機能と、（B）アクセスした匿名化ポリシーテーブルを使用して匿名化の要否を判定する機能と、（C）判定した匿名化の要否情報をセッション管理手段 122 に出力する機能と、を備えている。

[0042] 図 3 は、匿名化ポリシーテーブルの一例を示す表である。図に示すように、匿名化ポリシーテーブルは、パケットに含まれる幾つかの情報と、匿名化の要否の情報とが対応付けられたテーブルである。匿名化ポリシーテーブルは、ユーザが事前に設定することを想定するが、ネットワーク上のノード（アンカーサーバ 200 など）が動的に設定するものとしても良い。尚、図において、匿名化ポリシーテーブルの“any”は、対応する項目が何であっても良いことを示し、匿名化の要否の判定に際しては、エントリ番号（No）の小さい値から順に評価する。

[0043] 図 2 に戻って説明を続ける。セッション管理手段 122 は、セッションの開始及び終了を判定する機能と、情報記録装置 140 に記録されたセッション管理テーブルを管理する機能と、を備えている。本実施の形態 1 では、セッションとして TCP セッションを想定しており、TCP セッションは、宛先アドレスと、送信元アドレスと、宛先ポート番号と、送信元ポート番号と、に基づいて識別される。尚、TCP セッションに限定されず、他の単位をセッションとみなしても良い。

[0044] セッション管理手段 122 は、匿名性確保要否判定手段 121 から匿名化が必要であるとの情報が入力された場合に、インタフェース 110A から入力されたパケットを匿名化確保の対象のパケットとして、セッション管理処理を実施する。ここで、セッション管理とは、セッションの開始及び終了を判定し、さらに、匿名アドレス選択手段 123 と匿名アドレス生成手段 124 が生成した匿名アドレスを使用して、情報記録装置 140 に記録されたセ

セッション管理テーブルのエントリ作成及び削除と、内容の更新とを実施することをいう。図4に、セッション管理テーブルの一例を示す。以下、セッション管理手段122が行うセッション管理処理について、より具体的に説明する。

[0045] まず、本実施の形態1では、セッションとしてTCPセッションを想定しているため、セッション管理手段122は、TCPのSYNパケットを用いてセッションの開始を検出することができる。

[0046] 次に、セッション管理手段122は、セッションの開始を検出した場合には、TCPセッションを識別するための情報を検索キーとしてセッション管理テーブルを検索し、同一のセッションが既に存在するか否かを検索する。検索の結果、同一のセッションが存在しなかった場合には、セッション管理手段122は、新規セッションの開始であるものと判定し、匿名アドレス選択手段123に匿名アドレスの割当てを要求する。

[0047] 次に、セッション管理手段122は、匿名アドレスの割当て要求の結果と、匿名アドレスと、匿名アドレスを用いて到達性のあるアンカーサーバ200のアドレスと、を取得した場合に、受信パケットから抽出した宛先アドレスと、送信元アドレスと、宛先ポート番号と、送信元ポート番号と、プロトコル種別と、匿名アドレスと、匿名アドレスを用いて到達性があるアンカーサーバ200のアドレスと、を用いて新たなエントリを生成し、生成したエントリをセッション管理テーブルに追加する。また、セッション管理手段122は、予め決定しておいた有効時間を現在時刻に加算した時刻を、追加するエントリの失効時刻として設定する。

[0048] そして、セッション管理手段122は、受信したパケットが、セッション管理テーブルにエントリを有するセッションに属するパケットである場合には、対応するエントリの失効時刻の更新を行う。失効時刻の更新方法としては、例えば、最初の失効時刻を算出する際に使用したのと同じ有効時間を、パケットを受信した時刻に加算することで、更新後の失効時刻を求めるものとしても良いし、これに限定されず、他の異なる時間を受信時刻に加算する

ようにしても良い。

[0049] また、セッション管理手段 122 は、セッションの終了を検出して、セッション管理テーブルから対応するエントリを削除する。例えば、TCPセッションの場合には、FIN パケット、ACK+FIN パケット、FIN パケットという一連の TCP セッションの終了手順や、RST パケットを検出することで、セッションの終了の判定を行うことができる。FIN パケットなどを用いて TCP セッションの終了判定を行う場合には、一連のパケットの到着を記憶しておく必要があるが、TCP セッションの終了判定処理自体は、TCP を処理するスタックはもとより、広く適用された一般的な技術である。このため、TCP セッションの終了判定処理については、その詳細な構成及び動作の説明を省略する。

[0050] さらに、セッション管理手段 122 は、セッション管理テーブルを定期的に監視して、失効時刻が現在時刻よりも過去となったエントリを、セッション管理テーブルから削除する。

[0051] 図 2 に戻って説明を続ける。匿名アドレス選択手段 123 は、セッション管理手段 122 から匿名アドレスの割当てを要求された場合に、通信ノード 300 のアドレスの匿名性を確保するためのプレフィクスを決定する。そして、匿名アドレス選択手段 123 は、決定したプレフィクスを基にして、匿名アドレス生成手段 124 に匿名アドレスの生成を依頼することで、匿名アドレスを取得する。匿名アドレス選択手段 123 は、セッション管理手段 122 からの匿名アドレス割当て要求への応答として、匿名アドレスと、匿名アドレスを用いて到達性のあるアンカーサーバ 200 のアドレスと、をセッション管理手段 122 に応答する。

[0052] 匿名アドレス選択手段 123 は、匿名アドレスの基となるプレフィクスを決定するに際して、情報記録装置 140 に記録されたプレフィクス情報テーブルの情報をを用いる。以下、プレフィクス情報テーブルについて、より具体的に説明する。

[0053] 図 5 は、プレフィクス情報テーブルの一例を示す表である。図に示すよう

に、プレフィクス情報テーブルは、アンカーサーバアドレスと、プレフィクスセット番号と、プレフィクスと、I I D (Interface Identifier) K e y と、割当状態と、割当終了時刻と、失効時刻と、についての情報を有している。尚、図に示したプレフィクス情報テーブルは一例であり、上述した項目の一部を含む構成や、他の情報を含む構成としても良い。以下、プレフィクス情報テーブルが含む各情報について説明する。

[0054] アンカーサーバアドレスは、匿名アドレスを用いて到達性のあるアンカーサーバ200のアドレスである。また、アンカーサーバアドレスは、匿名アドレスを生成する際に使用するプレフィクスについて、プレフィクスの基本的な取得先としたアンカーサーバ200のアドレスである。尚、アンカーサーバ200のこれら2種類のアドレスを区別する場合には、個々のアドレスを記録できるようにしても良い。

[0055] また、図5に示すプレフィクス管理テーブルでは、2つのアンカーサーバ200のアドレスが設定された例を示しているが、設定されるアンカーサーバ200のアドレスは1つであっても良いし、2つより多くのアンカーサーバ200のアドレスを使用するものとしても良い。1台のアンカーサーバ200を用いて匿名化装置100に複数のプレフィクスを割当てることができるが、割り当てるプレフィクスはアンカーサーバ200に到達性を有するものである必要がある。このため、1台のアンカーサーバ200が提供可能なプレフィクスのバリエーションには限界がある。また、1台のアンカーサーバ200では、耐障害性の面でも問題がある。従って、より高い匿名性や耐障害性を確保するとの観点から、複数のアンカーサーバ200を適用するのが好適である。

[0056] プレフィクスセット番号は、アンカーサーバ200から取得したプレフィクス群に割当てられた、プレフィクスセット番号である。尚、プレフィクスセット番号は必ずしも必要ではないが、アンカーサーバ200に新しいプレフィクス群を割当ててもらう場合に、既に取得しているプレフィクス群が提示される際は、プレフィクスセット番号を適用することで、匿名化装置100

0が、アンカーサーバ200に提示する際の情報量を削減することができる。換言すると、匿名化装置100は、既に取得したプレフィクス群を個別にアンカーサーバ200に通知する必要が無く、プレフィクスセット番号のみを送信するだけで良い。

[0057] プレフィクスは、アンカーサーバ200から取得したプレフィクス情報である。本実施の形態1では、匿名アドレス生成手段124が、アンカーサーバ200から取得したプレフィクスとIID (Interface Identifier) とを合わせて匿名アドレスを生成するものとして説明するが、匿名アドレスをアンカーサーバ200から直接取得するものとしても良い。匿名アドレスをアンカーサーバ200から直接取得する場合には、後述するIID Keyは必要としない。尚、IPv6アドレスは、上位64bitのプレフィクス部と下位64bitのIID部を合わせて、128bitのアドレスとなる。

[0058] IID Keyは、IPv6アドレスのIID部を生成する際に使用するKey情報である。尚、IID部の生成手順の詳細については後述する。

[0059] 割当状態は、特定のセッションにプレフィクスが割当て済みであるか否かを示す。割当状態が'Y'の場合には割当て済みであることを示し、'N'の場合には未割当てであることを示す。

[0060] 割当終了時間は、セッションが終了して、セッションに割当てたプレフィクスが開放された時刻を示す。

[0061] 失効時刻は、プレフィクスが無効となる時刻を示す。特定のセッションに割当てるプレフィクスを選択する際には、失効時刻が現在の時刻よりも未来の時刻であるプレフィクスを選択する。特定のセッションに割当て中のプレフィクスの失効時刻が経過した場合に、プレフィクスを無効にしてしまうと通信途絶が発生する。このため、特定のセッションに割当て中のプレフィクスは、割当てが完了するまでの間は無効としない。尚、通信途絶しても良い場合には、割当て中か否かに関わらず無効にするものとしても良い。

[0062] 匿名アドレス選択手段123は、セッション管理手段122から匿名アドレスの割当てを要求された場合に、プレフィクス情報テーブルに記録された

エントリのうち、割当状態が'N'（即ち、未割当て）であり、かつ、失効時刻に設定された時刻が現在の時刻よりも未来であるエントリを選択候補として、この選択候補のエントリから適切なプレフィクスを1つ選択する。尚、適切なプレフィクスの選択手順の詳細については後述する。

[0063] 匿名アドレス選択手段123は、適切な1つのプレフィクスを選択した後に、選択したプレフィクスとエントリのI I D K e y情報とを匿名アドレス生成手段124に出力して、その結果として、匿名アドレスを取得する。取得した匿名アドレスは、セッション管理手段122に応答される。同時に、匿名アドレス選択手段123は、プレフィクス情報テーブルにおいて、選択したプレフィクスのエントリを割当て済みに更新する（即ち、割当状態を'Y'にする）。尚、アンカーサーバ200から取得するプレフィクスは、128 b i tのアドレスそのものとして取得が可能であるが、プレフィクスを128 b i tのアドレスそのものとして取得する場合には、匿名アドレス生成手段124の機能は用いずに、アンカーサーバ200から割当てられたアドレスをそのまま応答する。

[0064] また、匿名アドレス選択手段123は、プレフィクスの選択を試行した結果、適切なプレフィクスを発見できなかった場合に、新たなプレフィクスを要求するためのプレフィクス要求信号を、アンカーサーバ200に送信する機能を備えている。プレフィクス割当要求信号には、割当て要求先とするアンカーサーバ200が管理するプレフィクスであり、かつ、既に保持しているプレフィクスを提示するための情報を格納する。この情報としては、通信帯域の効率を考慮し、プレフィクスセット番号を使用する。尚、プレフィクスセット番号を使用せずに、個別のプレフィクスを直接格納するものとしても良い。

[0065] また、匿名アドレス選択手段123は、要求するプレフィクスセットの数（或いは、プレフィクスの数）と、匿名化装置100のアドレスと、をプレフィクス割当要求信号に格納する。匿名化装置100のアドレスは、プレフィクス割当要求信号の送信元アドレスにも設定されるため、必ずしも別途格

納する必要はないが、送信元アドレスとは異なるアドレスに設定が可能である場合などには、必要に応じて格納するものとする。また、上述した情報以外の情報をプレフィクス割当要求信号に格納するものとしても良い。

[0066] 匿名アドレス選択手段 123 は、プレフィクス割当要求信号の応答として、アンカーサーバ 200 から応答されたプレフィクス割当応答信号を受信した場合には、受信したプレフィクス割当応答信号に含まれる情報を使用して、プレフィクス情報テーブルにエントリを追加する。

[0067] プレフィクス割当応答信号には、割当られたプレフィクスセット番号と、プレフィクスセット番号に属するプレフィクスと、プレフィクスに関連付けられた I I D K e y 及び失効時刻と、アンカーサーバ 200 のアドレスと、が格納される。アンカーサーバ 200 のアドレスは必ずしも必要ではないが、例えば、匿名化アドレスを用いて到達性のあるアンカーサーバ 200 のアドレスと、プレフィクス割当要求信号の送信先としたアンカーサーバ 200 のアドレスと、が異なる場合などには必要となる。また、上述した情報以外の情報をプレフィクス応答信号に格納するものとしても良い。

[0068] 尚、プレフィクス割当要求信号の送信先とするアンカーサーバ 200 のアドレスは、事前に設定されることを想定するが、他の方法を用いて取得するものとしても良い。また、アンカーサーバ 200 のアドレスは、複数のアドレスが設定可能であることを想定するが、複数のアドレスを設定する場合には、プレフィクス割当要求信号の送信先とするアンカーサーバ 200 として、例えば、複数のアンカーサーバ 200 のアドレスのうちからランダムに 1 つ選択する方法が考えられる。

[0069] 尚、プレフィクス割当要求信号及びプレフィクス割当応答信号は、秘匿性や完全性といったセキュリティが確保されることが必要である。セキュリティ確保手段としては、I P s e c などの一般的な技術を使用することができる。

[0070] 図 2 に戻って説明を続ける。匿名アドレス生成手段 124 は、匿名アドレス選択手段 123 からの依頼に応じて匿名アドレスを生成する機能を備えて

いる。匿名アドレス生成手段 124 は、生成した匿名アドレスを、匿名アドレス選択手段 123 に応答する。以下、匿名アドレス生成手段 124 が行う匿名アドレスの生成手順を例示する。尚、以下の例では、匿名アドレス生成手段 124 は、匿名アドレスを生成する際に、匿名アドレス選択手段 123 から出力されたプレフィクス情報や `IID Key` を使用する。また、匿名アドレス生成手段 124 は、匿名化制御手段 120 に入力されたパケットの送信元ポート番号についても使用する。

[0071] まず、匿名アドレス生成手段 124 は、以下の式 1 を用いて `Key` を算出する。尚、式 1 においては、`IID Key` を `IID_key` として表示する。

$$Key = \text{Extract}(n, H(\text{IID_key}, \text{src_port} \parallel \text{FIXED_DATA})) \cdots (\text{式 1})$$

[0072] 式 1 において、 $H(k, x)$ は、キー k を使用してデータ x にハッシュ処理を施す処理を示す。ハッシュ処理アルゴリズムとしては、例えば、`HMAC-MD5` や、`HMAC-SHA-1` などを使用することができる。勿論、他のハッシュアルゴリズムを使用するものとしても良い。

[0073] `src_port` は、パケットの送信元ポート番号を示す。`FIXED_DATA` は、任意の固定データを示す。記号 `'|'` は、ここでは、記号の前後の 2 つのデータをそれぞれバイト列の情報であるとみなして、それら 2 つのデータを連結することを意味する。

[0074] $\text{Extract}(n, x)$ は、データ x の上位から n ビット分のデータを抜き出す処理を示す。 n の値は、ハッシュアルゴリズムとして `HMAC-MD5` を適用する場合には 128 とし、`HMAC-SHA-1` を適用する場合には 160 とすると好適であるが、異なる値にしても良い。

[0075] 式 1 の処理では、セッション毎（即ち、送信ポート番号が変わる度）に `Key` の値を変更する。これにより、仮に同じ `IID Key` を使う場合においても、異なる匿名アドレスを生成できるようにするために、式 1 での処理を実施する。従って、別途 `IID Key` を更新する仕組みを適用した場合

などには式1の計算を行わずに、 IID_Key をそのまま Key として使用するものとしても良い（即ち、 $Key = IID_key$ ）。

[0076] 次に、匿名アドレス生成手段124は、以下の式2を用いて匿名アドレスの IID 部（即ち、 $IPv6$ アドレスの下位64bit部分）を算出する。

$$Derived\ IID = Extract(64, E(Key, CPE_IID)) \dots \text{(式2)}$$

[0077] 式2において、 Key は式1で求めた値を示す。 CPE_IID は、匿名化装置100の識別子を示す。 CPE_IID としては、アンカーサーバ200を管理するオペレータから割当てられた識別番号或いは識別文字列の使用を想定する。匿名化装置100のインタフェース110Bにオペレータがアドレスを割当てた場合には、割り当てたアドレスを CPE_IID として使用するものとしても良い。

[0078] 最後に、匿名アドレス生成手段124は、式2で求めた $Derived\ IID$ と、匿名アドレス選択手段123から出力されたプレフィクス情報と、を結合して匿名アドレスを構成する。

[0079] ここで、重要なポイントは、匿名アドレスと、匿名アドレスを割当てた匿名化装置100と、の対応関係を示す情報が存在しない場合において、匿名アドレスやポート番号といったサーバ400の管理者が取得し得る情報（即ち、サーバ400が受信したパケットに含まれる情報）を用いて、アンカーサーバ200を管理するオペレータが、 $Derived\ IID$ を算出できるようにすることである。

[0080] この結果、例えば、匿名化装置100とアンカーサーバ200の機能を用いて匿名通信を行う通信ノード300が、サーバ400に不正アクセスを行った場合には、アンカーサーバ200を管理する（即ち、匿名性確保サービスを実施する）オペレータに対して、不正アクセスのログに残された匿名化アドレスや、（送信元ポート番号を使用する場合の）送信元ポートを通知することで、オペレータは、不正アクセスを実施した通信ノード300が接続する匿名化装置100を割出すことができる。

- [0081] 従って、本実施の形態 1 に係る通信システム 1 によれば、通信ノード 300 の通信の匿名性を確保することができると共に、さらに、不正アクセスなどの問題が発生した場合において、匿名アドレス（及び送信元ポート番号）を用いた追跡性についても確保することが可能となる。
- [0082] 尚、匿名アドレスの算出方法は上述した方法に限定されず、他の異なる手段を用いて匿名アドレスを算出するものとしても良い。また、上述したように、匿名アドレスをアンカーサーバ 200 から直接取得することができる場合には、匿名アドレス生成手段 124 が匿名アドレスを生成しなくとも良い。また、匿名アドレスの I I D 部の算出方法については、匿名化装置 100 は、アンカーサーバ 200 から取得した情報（例えば I I D__k e y）を用いずに、匿名化装置 100 自らが I I D 部を算出するものとしても良い。従って、匿名化装置 100 は、アンカーサーバ 200 から匿名アドレスを直接取得する場合には、匿名アドレス生成手段 124 を備えていなくとも良い。また、匿名化装置 100 が匿名アドレス生成手段 124 を備えて自ら匿名アドレスを生成する場合には、プレフィックスのみをアンカーサーバ 200 から取得するものとしても良いし、プレフィックスと I I D 部を生成するための情報（例えば I I D__k e y）とを取得するものとしても良い。
- [0083] 図 2 に戻って説明を続ける。パケット処理手段 130 は、インタフェース 110 A で受信されたパケットが匿名化制御手段 120 を経由して入力された場合に、入力されたパケットの宛先アドレスと、送信元アドレスと、宛先ポート番号と、送信元ポート番号と、を検索キーとして、情報記録装置 140 に保持されたセッション管理テーブルを検索する。検索の結果、該当するエントリを発見した場合には、パケット処理手段 130 は、入力されたパケットの送信元アドレスを、検索されたエントリに設定された匿名アドレスに書き換える処理を実施する。
- [0084] そして、パケット処理手段 130 は、匿名アドレスに書き換えたパケットについてカプセル化を実施する。カプセル化の際には、外側の I P ヘッダの送信元アドレスとして、匿名化装置 100 自身の有するアドレスを使用し、

宛先アドレスとして、検索されたエントリのアンカーサーバ200のアドレスを使用する。カプセル化されたパケットは、インタフェース110Bを経由してネットワーク600へと送出される。尚、匿名化装置100自身の有するアドレスとしては、インタフェース110Bに割当てられたIPアドレスを想定するが、このアドレスに限定されるものではない。

[0085] さらに、パケット処理手段130は、インタフェース110Bからパケットが入力された場合に、入力されたパケットがカプセル化されたパケットであるか否かをチェックする。そして、カプセル化されたパケットであった場合には、パケット処理手段130は、外側IPヘッダの宛先アドレス及び送信元アドレスと、内側IPヘッダの宛先アドレス及び送信元アドレスと、宛先ポート番号と、送信元ポート番号と、を検索キーとして、情報記録装置140に記録されたセッション管理テーブルを検索する。

[0086] パケット処理手段130は、インタフェース110Bから受信したパケットに対して検索を実施する場合には、以下の対応を用いて検索を行う。

受信パケットの外側IPヘッダ 宛先アドレス

⇒匿名化装置100のアドレス

受信パケットの外側IPヘッダ 送信元アドレス

⇒セッション管理テーブル アンカーサーバアドレス

受信パケットの内側IPヘッダ 宛先アドレス

⇒セッション管理テーブル 匿名アドレス

受信パケットの内側IPヘッダ 送信元アドレス

⇒セッション管理テーブル 宛先アドレス

受信パケットの宛先ポート番号

⇒セッション管理テーブル 送信元ポート番号

受信パケットの送信元ポート番号

⇒セッション管理テーブル 宛先ポート番号

[0087] パケット処理手段130は、上記の対応関係を用いてセッション管理テーブルを検索した結果、該当するエントリを発見した場合には、まず、デカプ

セル化処理を実施する。そして、デカプセル化処理に続いて、パケット処理手段１３０は、内側のＩＰヘッダの宛先アドレスを、匿名アドレスから、検索されたエントリの送信元アドレスとして記録されたアドレスへと書き換える。換言すると、パケット処理手段１３０は、パケットのアドレスを、匿名アドレスから通信ノード３００のアドレスへと戻す処理を実施する。さらに、パケット処理手段１３０は、宛先アドレスが通信ノード３００のアドレスへと戻されたパケットを、インタフェース１１０Ａから送出する。この結果、パケット処理手段１３０が送出したパケットを、ローカルネットワーク５００に接続した通信ノード５００が受信する。

[0088] 図２に戻って説明を続ける。情報記録装置１４０は、図３に示した匿名化ポリシテーブルと、図４に示したセッション管理テーブルと、図５に示したプレフィクス情報テーブルと、を記録した記録装置である。

[0089] 図１に戻って説明を続ける。アンカーサーバ２００は、匿名化装置１００からのプレフィクス割当要求を受信した場合に、要求に応じてプレフィクスを匿名化装置１００に割当て、割当てたプレフィクスを格納したプレフィクス応答信号を、匿名化装置１００に応答する機能を備えている。

[0090] また、アンカーサーバ２００は、トンネリングを用いて匿名化装置１００からアンカーサーバ２００に転送されたパケットを、デカプセル化する機能を備えている。ここで、デカプセル化されたパケットは、一般的なルータと同様の処理を用いて、転送処理される。また、アンカーサーバ２００は、匿名アドレス宛に送信されたパケットを受信した場合には、受信したパケットをカプセル化して匿名化装置１００に転送する機能を備えている。

[0091] 図６は、アンカーサーバ２００を示す構成図である。アンカーサーバ２００は、インタフェース２１０と、プレフィクス割当手段２２０と、転送手段２３０と、プレフィクス記録装置２４０と、転送情報記録装置２５０と、を備えている。

[0092] インタフェース２１０は、ネットワーク６００に接続され、ネットワーク６００に接続された他のノード（匿名化装置１００やサーバ４００など）と

パケットの送受信を行う機能を備えている。インタフェース 210 は、受信したパケットがプレフィクス割当要求信号であった場合、プレフィクス割当手段 220 にパケットを出力し、それ以外のパケットであった場合には、転送手段 230 に出力する。また、プレフィクス割当手段 220 から応答されたプレフィクス割当応答信号や、転送手段からネットワーク 600 へと送られるパケットは、インタフェース 210 を介してネットワーク 600 へと送信される。

[0093] プレフィクス割当手段 220 は、プレフィクス割当要求信号を受信した場合に、(A) プレフィクス記録装置 240 に記録された貸出しプレフィクステーブルにアクセスする機能と、(B) プレフィクス割当要求信号に格納された情報に基づき適切なプレフィクスを選択する機能と、(C) プレフィクスセット番号と、プレフィクスセットに属するプレフィクス群と、各プレフィクスに関連付けられた I I D K e y と、失効時刻を格納したプレフィクス割当応答信号と、を応答する機能と、を備えている。

[0094] プレフィクス割当要求信号には、匿名化装置 100 が既に保持しているプレフィクスの情報として、1 つ乃至複数のプレフィクスセット番号と、要求するプレフィクスセットの数と、が格納されることを想定する。尚、匿名化装置 100 が保持しているプレフィクスの情報を示す場合には、プレフィクスセットとしてではなく、プレフィクス自体を格納するものとしても良い。また、要求するプレフィクスの数についても、プレフィクスセットの数ではなく、プレフィクス自体の数としても良い。さらに、プレフィクス割当要求信号には、上述した情報の一部のみを含むものとしても良いし、上述した情報を全く含まない構成としても良い。

[0095] プレフィクス割当手段 220 は、匿名化装置 100 に割当てするプレフィクスを選択する場合に、プレフィクス割当応答信号に格納されたプレフィクスセット或いはプレフィクスに該当しないプレフィクスを選択する。ここで、選択するプレフィクスの数は、プレフィクスセット或いはプレフィクスを要求された数とする。

- [0096] 図7は、貸出しプレフィクステーブルを示す表である。図に示すように、貸出しプレフィクステーブルは、プレフィクスセット番号と、プレフィクスと、プレフィクスに対応付けられた I I D K e y の情報と、を含む。尚、貸出しプレフィクステーブルは、これらの情報に加えて、他の情報を含むものとしても良い。例えば、本実施の形態1では、失効時刻を算出する際に、プレフィクスに関わらず、事前に決められた有効時間を現在時刻に加えることで失効時刻を算出するものと想定するが、プレフィクス毎に異なる有効時間を設ける場合には、各プレフィクスに対応した有効時間を貸し出しプレフィクステーブルに含めるものとして良い。
- [0097] 図6に戻って説明を続ける。転送手段230は、インタフェース210から入力されたデータパケットを調査し、カプセル化されたパケットであった場合には、さらに、外側IPヘッダの送信元アドレス及び宛先アドレスと、内側IPヘッダの送信元アドレスと、を読み出す。そして、転送手段230は、外側IPヘッダの宛先アドレスが、アンカーサーバ200自身のアドレスと一致することを確認した後に、さらに、内側IPヘッダの送信元アドレスのプレフィクス部が、プレフィクス記録装置240に記録された貸出しプレフィクステーブルに存在するか否かの確認を行う。
- [0098] そして、転送手段230は、外側IPヘッダの宛先アドレスがアンカーサーバ200のアドレスと一致し、かつ、内側IPヘッダの送信元アドレスのプレフィクス部が貸出しプレフィクステーブルに存在する場合には、入力されたパケットの外側IPヘッダの送信元アドレスと、内側IPヘッダの送信元アドレスと、の対応（即ち、匿名化装置100のアドレスと匿名アドレスとの対応）を保持するために、転送情報記録装置250に記録された転送テーブルにエントリを追加する。ここで、転送手段230は、エントリを追加する際に、それら2つのアドレスの対応関係が失効する時刻についても記録する。尚、同じエントリが転送テーブルに既に存在する場合には、後述するように、失効時刻のみを更新する。
- [0099] 図8は、転送テーブルを示す表である。転送テーブルの失効時刻には、事

前に決定しておいた有効時間をエントリ作成時の時刻に加算した時刻が設定される。この失効時刻は、作成されたエントリに対応するパケット（即ち、匿名化装置１００からトンネリングされたパケットや、匿名アドレス宛に送信されたパケットなど）を処理する都度、更新される。

[0100] 転送手段２３０は、転送テーブルへのエントリの追加或いは更新を行った後に、入力されたパケットをデカプセル化して、一般的なＩＰルーティングを用いた、転送処理を実施する。

[0101] また、転送手段２３０は、インタフェース２１０から入力されたデータパケットを調査し、カプセル化されていないパケットであった場合には、さらに、転送情報記録装置２５０に記録された転送テーブルのエントリについて、入力されたパケットのＩＰヘッダの宛先アドレスと一致する匿名アドレスが設定されたエントリが存在するか否かを検索する。検索の結果、一致するエントリを発見した場合には、入力されたパケットについてカプセル化処理を実施する。カプセル化処理の際には、外側ＩＰヘッダの宛先アドレスには、一致したエントリの匿名化装置１００のアドレスが使用され、外側ＩＰヘッダの送信元アドレスには、アンカーサーバ２００自身のアドレスが使用される。カプセル化処理に続いて、転送手段２３０は、カプセル化後のパケットに対して、一般的なＩＰルーティングを使用した、転送処理を実施する。

[0102] 尚、本実施の形態１におけるアンカーサーバ２００は、プレフィクスを割当てる機能と、匿名アドレスからのパケットや匿名アドレス宛のパケットを転送する機能と、を備えるものとして説明したが、これら２つの機能を異なるサーバでそれぞれ実施する構成としても良い。各機能を異なるサーバで実施する構成とする場合には、プレフィクスの割当機能を担うサーバが、インタフェース２１０と、プレフィクス割当手段２２０と、プレフィクス記録装置２４０と、を備える構成とし、匿名アドレスを有するパケットを転送する機能を担うサーバが、インタフェース２１０と、転送手段２３０と、転送情報記録装置２５０と、を備える構成とすれば良い。

[0103] 図６に戻って説明を続ける。プレフィクス記録装置２４０は、図７に示し

た貸出しプレフィクステーブルを保持する記録装置である。

[0104] 転送情報記録装置 250 は、図 8 に示した転送テーブルを保持する記録装置である。

[0105] 図 1 に戻って説明を続ける。通信ノード 300 は、匿名化装置 100 を介して、後述するネットワーク 600 上の他のノードにアクセスすることができる。尚、通信ノード 300 は、IP に従った通信機能を備えた一般的な通信ノードであるため、その詳細な構成及び動作の説明を省略する。

[0106] サーバ 400 は、WEB サービスなどを提供するサーバである。サーバ 400 は、IP に従った通信機能を備えた一般的なサーバであるため、その詳細な構成及び動作の説明を省略する。

[0107] ローカルネットワーク 500 は、匿名化装置 100 と通信ノード 300 とが接続されたネットワークである。ローカルネットワーク 500 としては、企業内ネットワークや家庭内ネットワークといった、いわゆる LAN (Local Area Network) を想定するが、LAN に限定されず、他のネットワークでも良い。

[0108] ネットワーク 600 は、匿名化装置 100 と、アンカーサーバ 200 と、サーバ 400 と、が接続するネットワークである。ネットワーク 600 は、ISP (Internet Service Provider) が提供するネットワークやインターネットを含んだ広域ネットワークである。

[0109] 尚、上述したインタフェース 110A と、インタフェース 110B と、インタフェース 210 と、は、例えば、LAN カードなどの NIC (Network Interface Card) と、NIC を動作させるソフトウェア (ドライバ) と、から構成することができる。

[0110] 尚、上述した匿名化制御手段 120 と、パケット処理手段 130 と、プレフィクス割当手段 220 と、転送手段 230 と、は、いずれもソフトウェアを用いてその機能を実現することができる。さらに、これら手段のいずれか一部或いは全てを、ハードウェアを用いて構成することも可能である。

[0111] また、上述した情報記録装置 140 と、プレフィクス記録装置 240 と、

転送情報記録装置 250 と、は、情報を記録可能な装置（半導体メモリやハードディスクドライブなど）を用いて構成することができる。

[0112] 尚、図 1 乃至図 8 に示した各手段や装置の構成は例示にすぎず、本発明の趣旨を逸脱しない範囲で他の構成を用いて実現するものとしても良い。

[0113] （動作の説明）

次に、図 9 乃至図 18 を参照して、本実施の形態 1 に係る通信システム 1 の動作について説明する。図 9 乃至図 12 は、通信ノード 300 からパケットを受信した場合の、匿名化装置 100 の動作を示すフローチャートである。図 13 及び図 14 は、アンカーサーバ 200 の動作を示すフローチャートである。図 15 乃至図 18 は、通信ノード 300 がサーバ 400 との通信を開始してから完了するまでの間の一連の処理の流れを説明するための図である。

[0114] 図 9 において、まず始めに、匿名化装置 100 の匿名化制御手段 120 は、通信ノード 300 が送信したパケットを、インタフェース 110A を介して受信する（ステップ S101）。そして、匿名性確保要否判定手段 121 は、受信パケットに対して匿名性を確保する必要があるか否かを判定する（ステップ S102）。ここで、匿名性が必要と判定された場合（即ち、'Y' の場合）には、ステップ S103 へと進む。一方で、匿名性を確保する必要がないと判定された場合（即ち、'N' の場合）には、ステップ S110 へと進む。

[0115] 次に、セッション管理手段 122 は、ステップ S103 で匿名性が必要と判定された場合には、受信パケットの内容をチェックし、セッションの開始であるか否かを判定する（ステップ S103）。セッションが TCP セッションである場合には、上述したとおり、パケットが SYN パケットであるか否かに応じてセッションの開始を判定することができる。また判定の際に、セッション管理手段 122 は、セッション管理テーブルに、セッションを一意に識別するための情報が一致するエントリが存在しないことも確認する。重複したエントリが存在する場合には、セッション管理手段 122 は、セッ

セッションの開始であるものとは判定しない。ここで、セッションの開始であると判定された場合（即ち、'Y'の場合）には、ステップS 104へと進む。一方で、セッションの開始でないと判定された場合（即ち、'N'の場合）には、ステップS 107へと進む。

[0116] 次に、匿名アドレス選択手段123は、ステップS 104でセッションの開始であると判定された場合には、匿名アドレスを生成する際に使用するプレフィクスを選択する（ステップS 104）。尚、匿名アドレス選択手段123が行うステップS 104での処理の詳細については、図10を参照して後述する。

[0117] 次に、匿名アドレス生成手段124は、選択したプレフィクスから匿名アドレスを生成する（ステップS 105）。

[0118] 次に、セッション管理手段122は、匿名アドレスと、ステップS 101における受信パケットから取得した、セッションを識別するための情報と、匿名アドレスを用いて到達性のあるアンカーサーバ200のアドレス（即ち、匿名アドレスを構成する際に使用したプレフィクスの取得元のアンカーサーバ200のアドレス）と、を用いて、セッション管理テーブルに新規なエントリを作成する（ステップS 106）。ステップS 106での処理が終了した後、ステップS 110へと進む。

[0119] また、セッション管理手段122は、ステップS 103でセッションの開始でないと判定した場合には、セッションの終了判定を行う（ステップS 107）。上述したように、セッションがTCPセッションである場合には、FINパケット、ACK+FINパケット、FINパケットという一連のTCPセッション終了の手順や、RSTパケットを検出することで、セッション終了の判定を行うことができる。ここで、セッションの終了であると判定された場合（即ち、'Y'の場合）には、ステップS 108へと進む。一方で、セッションの終了でないと判定された場合（即ち、'N'の場合）には、ステップS 109へと進む。

[0120] 次に、セッション管理手段122は、ステップS 107でセッションの終

了であると判定された場合には、セッション終了時の処理を行う（ステップ S 1 0 8）。具体的には、セッション管理手段 1 2 2 は、セッション管理テーブルから対応するエントリを削除し、プレフィクス情報テーブルの対応するエントリの割当状態を 'N'（未割当）とし、また、割当終了時刻を現在時刻に更新する。ステップ S 1 0 8 での処理が終了した後、ステップ S 1 1 0 へと進む。

[0121] また、セッション管理手段 1 2 2 は、ステップ S 1 0 7 でセッションの終了でないと判定された場合には、セッション管理テーブルの失効時刻を更新する（ステップ S 1 0 9）。ステップ S 1 0 9 での処理が終了した後、ステップ S 1 1 0 へと進む。

[0122] 最後に、パケット処理手段 1 3 0 は、セッション管理テーブルの情報を参照し、対応するエントリが存在する場合には受信パケットの送信元アドレスを匿名アドレスに書き換え、さらに、匿名アドレスを用いて到達性のあるアンカーサーバ 2 0 0 へとトンネリングするためのカプセル化処理を行う（ステップ S 1 1 0）。尚、パケット処理手段 1 3 0 が行うステップ S 1 1 0 での処理の詳細については、図 1 2 を参照して後述する。

[0123] 次に、図 1 0 を参照して、図 9 のステップ S 1 0 4 における処理の詳細について説明する。図 1 0 は、匿名化装置 1 0 0 の匿名アドレス選択手段 1 2 3 が行うプレフィクス決定処理の動作を示すフローチャートである。

[0124] 図 1 0 において、まず、匿名化装置 1 0 0 の匿名アドレス選択手段 1 2 3 は、プレフィクス情報テーブルを検索し、未割当のプレフィクスを抽出する（ステップ S 2 0 1）。ここで、未割当のプレフィクスが存在しないと判定された場合（即ち、'N' の場合）には、ステップ S 2 0 2 へと処理を進めて、後述するように、プレフィクス割当を要求する処理を行う。一方で、1 つ以上の未割当のプレフィクスが存在すると判定された場合（即ち、'Y' の場合）には、ステップ S 2 0 3 へと進む。

[0125] 次に、匿名アドレス選択手段 1 2 3 は、ステップ S 2 0 1 で未割当のプレフィクスが存在しないと判定された場合には、アンカーサーバ 2 0 0 に対し

てプレフィクス割当要求信号を送信することで、プレフィクス割当て処理を実施する（ステップS 2 0 2）。尚、匿名アドレス選択手段 1 2 3 が行うステップS 2 0 2での処理の詳細については、図 1 1を参照して後述する。そして、ステップS 2 0 2での割当要求処理の結果、新たなプレフィクスを取得した場合には、ステップS 2 0 4へと進む。

[0126] また、匿名アドレス選択手段 1 2 3は、ステップS 2 0 1で未割当のプレフィクスが存在すると判定された場合には、プレフィクス情報テーブルを検索し、アンカーサーバ 2 0 0から取得した後に一度も使用されていないプレフィクスを検索する（ステップS 2 0 3）。ここで、一度も使用されていないプレフィクスが存在すると判定された場合（即ち、' Y' の場合）には、ステップS 2 0 4へと進む。一方で、一度も使用されていないプレフィクスが存在しないと判定された場合（即ち、' N' の場合）には、ステップS 2 0 5へと進む。

[0127] ステップS 2 0 2でのプレフィクス割当て処理に続いて、或いは、ステップS 2 0 3で一度も使用されていないプレフィクスが存在すると判定された場合には、匿名アドレス選択手段 1 2 3は、一度も使用されていないプレフィクスのうちからランダムで1つのプレフィクスを選択し（ステップS 2 0 4）、プレフィクス決定処理を完了する。

[0128] また、匿名アドレス選択手段 1 2 3は、ステップS 2 0 3で一度も使用されていないプレフィクスが存在しないと判定された場合には、プレフィクス情報テーブルから、割当終了時刻が所定の時刻よりも過去のプレフィクスを検索する（ステップS 2 0 5）。所定の時刻は事前に設定することを想定する。ここで、該当するプレフィクスが存在しないと判定された場合（即ち、' N' の場合）には、ステップS 2 0 2へと進む。一方で、該当するプレフィクスが存在すると判定された場合（即ち、' Y' の場合）には、ステップS 2 0 6へと進む。

[0129] 次に、匿名アドレス選択手段 1 2 3は、所定の時刻よりも過去に割当てを終了したプレフィクスから、ランダムで1つのプレフィクスを選択し（ステ

ップS206)、プレフィクス決定処理を完了する。ここで、プレフィクスを選択する際には、割当終了時刻に応じて選択確率に重み付けを行うことで、より過去の割当終了時刻であるプレフィクスを、他のプレフィクスよりも選択され易くするといった処理を行うものとしても良い。

[0130] 尚、本実施の形態1で説明したプレフィクス決定処理は一例であり、他の方法を用いてプレフィクス決定処理を行うものとしても良い。例えば、プレフィクスが関連づけられたセッション情報(セッションがTCPセッションである場合には、パケットの送信元アドレス、宛先アドレス、送信元ポート番号、宛先ポート番号などの情報)の全て或いは一部の情報を予め記憶しておき、これらの情報と一致するセッションに対して、同じプレフィクスを割当てないようにする、或いは、割当てづらくするといった選択基準を設けるようにしても良い。

[0131] 次に、図11を参照して、図10のステップS202における処理の詳細について説明する。図11は、匿名化装置100の匿名アドレス選択手段123が行うプレフィクス割当要求処理の動作を示すフローチャートである。

[0132] 図11において、まず、匿名化装置100の匿名アドレス選択手段123は、匿名化装置100が既に保持しているプレフィクスであり、かつ、プレフィクス割当要求の対象とするアンカーサーバ200から取得したプレフィクスについて、プレフィクスセット番号と、割当要求するプレフィクスセットの数と、匿名化装置100のアドレスを設定したプレフィクス割当要求信号と、を構成する(ステップS301)。尚、上述したように、プレフィクスセット番号に代えてプレフィクス自体を設定するものとしても良い。また、割当要求するプレフィクスセットの数に代えて、要求するプレフィクスの数としても良い。

[0133] 次に、匿名アドレス選択手段123は、ステップS301において構成したプレフィクス割当要求信号を、アンカーサーバ200に送信する処理を行う(ステップS302)。

[0134] 次に、匿名アドレス選択手段123は、アンカーサーバ200から応答さ

れるプレフィクス割当応答信号を待つ（ステップS 3 0 3）。ここで、プレフィクス割当応答信号が受信された場合（即ち、' Y ' の場合）には、ステップS 3 0 4へと進む。プレフィクス割当応答信号が受信されていない場合（即ち、' N ' の場合）には、プレフィクス割当応答信号の受信を待つ。

[0135] 最後に、匿名アドレス選択手段 1 2 3 は、プレフィクス割当応答信号を受信した場合には、受信したプレフィクス割当応答信号の情報を使用して、プレフィクス情報テーブルに新たなエントリを追加する処理を行う（ステップS 3 0 4）。ステップS 3 0 4での処理が終了した後、図 1 0 に示したステップS 2 0 4へと進む。

[0136] 次に、図 1 2 を参照して、図 9 のステップS 1 1 0 における処理の詳細について説明する。図 1 2 は、匿名化装置 1 0 0 のパケット処理手段 1 3 0 が行うパケット処理の動作を示すフローチャートである。尚、パケット処理は、インタフェース 1 1 0 A が受信して、匿名化制御手段 1 2 0 が処理した後のパケットや、インタフェース 1 1 0 B が受信したパケットに対して行われる処理を示す。インタフェース 1 1 0 A が受信して、匿名化制御手段 1 2 0 が処理した後のパケットに対して行われる処理が、図 9 のステップS 1 1 0 で行われるパケット処理に相当する。

[0137] 図 1 2 において、まず、匿名化装置 1 0 0 のパケット処理手段 1 3 0 は、受信したパケットがカプセル化されているか否かを判定する（ステップS 4 0 1）。ここで、受信パケットがカプセル化されていると判定された場合（即ち、' Y ' の場合）には、ステップS 4 0 2へと進む。一方で、受信パケットがカプセル化されていないと判定された場合（即ち、' N ' の場合）には、ステップS 4 0 6へと進む。

[0138] 次に、パケット処理手段 1 3 0 は、ステップS 4 0 1 で受信パケットがカプセル化されていないと判定した場合には、受信したパケットに設定された情報を使用して、情報記録装置 1 4 0 に記録されたセッション管理テーブルを検索し（ステップS 4 0 2）、対応するエントリが存在するか否かを確認する（ステップS 4 0 3）。尚、ステップS 4 0 2 で検索を行う際に比較さ

れる情報は、上述したパケット処理手段 130 の説明において既に述べたため、ここではその説明を省略する。ステップ S 403 での確認の結果、対応するエントリが発見された場合（即ち、'Y' の場合）には、ステップ S 404 へと進む。一方で、発見されなかった場合（即ち、'N' の場合）には、ステップ S 410 へと進む。

[0139] 次に、パケット処理手段 130 は、ステップ S 403 で対応するエントリを発見した場合には、発見したエントリの匿名アドレスを使用して、受信したパケットの送信元アドレスを書き換える（ステップ S 404）。

[0140] 次に、パケット処理手段 130 は、ステップ S 404 で送信元アドレスを書き換えたパケットについて、アンカーサーバ 200 に転送するためのカプセル化処理を行う（ステップ S 405）。ステップ S 405 での処理が終了した後、ステップ S 410 へと進む。

[0141] 一方で、パケット処理手段 130 は、ステップ S 401 で受信パケットがカプセル化されていると判定した場合には、受信したパケット（カプセル化されたパケット）に設定された情報を使用して、情報記録装置 140 に記録されたセッション管理テーブルを検索し（ステップ S 406）、対応するエントリが存在するか否かを確認する（ステップ S 407）。尚、ステップ S 406 で検索を行う際に比較される情報は、上述したパケット処理手段 130 の説明において既に述べたため、ここではその説明を省略する。ステップ S 407 での確認の結果、対応するエントリが発見された場合（即ち、'Y' の場合）には、ステップ S 408 へと進む。一方で、発見されなかった場合（即ち、'N' の場合）には、ステップ S 410 へと進む。

[0142] 次に、パケット処理手段 130 は、ステップ S 407 で対応するエントリを発見した場合には、受信したパケットについて、デカプセル化を行う（ステップ S 408）。具体的には、パケット処理手段 130 は、受信したパケットの外側 IP ヘッダを除去する。

[0143] 次に、パケット処理手段 130 は、デカプセル化後のパケットの宛先アドレスを、セッション管理テーブルの送信元アドレスに記録されたアドレスに

書換える（ステップS 4 0 9）。このアドレス書換え処理のために、受信したパケットのアドレスが、匿名アドレスから通信ノード3 0 0のアドレスに書き戻されたことになる。ステップS 4 0 9での処理が終了した後、ステップS 4 1 0へと進む。

[0144] 最後に、パケット処理手段1 3 0は、通常のI Pルーティングの機能を用いてパケットをルーティングして、宛先アドレスに応じて、適切なインタフェースからパケットを送出する（ステップS 4 1 0）。例えば、ステップS 4 0 5でカプセル化されたパケットは、アンカーアドレス2 0 0宛であり、インタフェース1 1 0 Bからネットワーク6 0 0へと送出手される。また、例えば、ステップS 4 0 9でデカプセル化された後に、宛先アドレスが通信ノード3 0 0のアドレスに書換えられたパケットは、インタフェース1 1 0 Aからネットワーク5 0 0へと送出手される。

[0145] 次に、図1 3及び図1 4を参照して、アンカーサーバ2 0 0の動作について詳細に説明する。図1 3は、プレフィクス割当要求信号を受信した場合の、アンカーサーバ2 0 0のプレフィクス割当手段2 2 0が行うプレフィクス割当処理の動作を示すフローチャートである。

[0146] 図1 3において、まず、アンカーサーバ2 0 0は、プレフィクス割当要求信号を受信する（ステップS 5 0 1）。そして、アンカーサーバ2 0 0のプレフィクス割当手段2 2 0は、プレフィクス記録装置2 4 0に記録された貸出しプレフィクステーブルから、適切なプレフィクスを選択する（ステップS 5 0 2）。尚、プレフィクス割当手段2 2 0が行うプレフィクスの選択方法については、上述したプレフィクス割当手段2 2 0の説明において既に述べたため、ここではその説明を省略する。

[0147] 次に、プレフィクス割当手段2 2 0は、プレフィクス割当応答信号を構成する（ステップS 5 0 3では）。プレフィクス割当応答信号には、割当てられたプレフィクスセット番号と、プレフィクスと、I I D K e yと、プレフィクスの失効時刻と、アンカーサーバ2 0 0のアドレスと、が格納される。

- [0148] 最後に、プレフィクス割当手段220は、ステップS503で構成したプレフィクス割当応答信号を、プレフィクス割当要求信号の送信元である匿名化装置100に送信する（ステップ504）。
- [0149] 図14は、データパケットを受信した場合の、アンカーサーバ200の転送手段230が行うパケット転送処理の動作を示すフローチャートである。
- [0150] 図14において、まず、アンカーサーバ200の転送手段230は、受信したパケットがカプセル化されているか否かを判定する（ステップS601）。ここで、受信パケットがカプセル化されていると判定された場合（即ち、'Y'の場合）には、ステップ602へと進む。一方で、受信パケットがカプセル化されていないと判定された場合（即ち、'N'の場合）には、ステップS609へと進む。
- [0151] 次に、転送手段230は、ステップS601で受信パケットがカプセル化されていると判定した場合には、受信したパケット（カプセル化されたパケット）の外側IPヘッダの宛先アドレスが、アンカーサーバ200自身のアドレスであり、かつ、内側IPヘッダの送信元アドレスのプレフィクス部が、アンカーサーバ200が割当て用に保持しているプレフィクスに含まれているか否かを評価する（ステップS602）。評価の結果、受信したパケットの外側IPヘッダの宛先アドレスと内側IPヘッダの送信元アドレスについての条件を満たす場合（即ち、'Y'の場合）には、ステップS603へと進む。一方で、条件を満たさない場合（即ち、'N'の場合）には、ステップS608へと進む。
- [0152] 次に、転送手段230は、ステップS602において上述した条件を満たす場合には、受信パケットの内側IPヘッダの送信元アドレスを匿名アドレスとして、転送情報記録装置250に記録された転送テーブルを検索し（ステップS603）、対応するエントリが存在するか否かを確認する（ステップS604）。ステップS604での確認の結果、対応するエントリを発見した場合（即ち、'Y'の場合）には、ステップS605へと進む。一方で、発見しなかった場合（即ち、'N'の場合）には、ステップS606へと進む。

- 。
- [0153] 次に、転送手段230は、ステップS604で対応するエントリを発見した場合には、検索された転送テーブルのエントリの失効時刻を更新する（ステップS605）。一方で、転送手段230は、ステップS604で対応するエントリを発見しなかった場合（即ち、'N'の場合）には、転送テーブルに新たなエントリを追加する（ステップS606）。エントリを追加する際には、上述したように、受信パケットの内側IPヘッダの送信元アドレスを匿名アドレスとし、外側IPヘッダの送信元アドレスを匿名化装置100の項目とし、現在時刻に所定の時間を加えた値を失効時刻として設定する。
- [0154] 次に、転送手段230は、受信したパケットについて、デカプセル化処理を行う（ステップS607）。最後に、転送手段230は、通常のIPルーティングを用いて、デカプセル化したパケットの転送処理を実施する（ステップS608）。
- [0155] 一方で、転送手段230は、ステップS601で受信パケットがカプセル化されていないと判定した場合には、受信パケットの宛先アドレスを匿名アドレスとして、転送情報記録装置250に記録された転送テーブルを検索し（ステップS609）、対応するエントリが存在するか否かを確認する（ステップS610）。ステップS610での確認の結果、対応するエントリが発見された場合（即ち、'Y'の場合）には、ステップS611へと進む。一方で、発見されなかった場合（即ち、'N'の場合）には、ステップS608へと進む。
- [0156] 次に、転送手段230は、ステップS610で対応するエントリを発見した場合には、上述したステップS605での処理と同様にして、検索された転送テーブルのエントリの失効時刻を更新する（ステップS611）。
- [0157] 次に、転送手段230は、受信したパケットについて、検索されたエントリを使用してカプセル化を行う（ステップS612）。ステップS612での処理が終了した後、上述したステップS608へと進む。
- [0158] 次に、図15乃至図18を参照して、通信ノード300がサーバ400と

の通信を開始してから、サーバ400との通信が完了するまでの間の一連の処理を説明する。図15は、通信ノード300がサーバ400との通信を開始してから完了するまでの、匿名化装置100とアンカーサーバ200の各機能が行う処理を説明するためのシーケンス図である。尚、図15では、通信ノード300がサーバ400にWEBアクセスを実施する場合を例に説明する。また、匿名化装置100のアドレスをCPE__ADR1とし、アンカーサーバ200のアドレスをAnch__ADR1とし、通信ノード300のアドレスをCI__ADR1とし、サーバ400のアドレスをSv__ADR1として説明する。

[0159] 図15のステップS701において、まず、通信ノード300は、サーバ400のFQDN (Fully Qualified Domain Name) から、サーバ400のIPアドレスを解決する。尚、サーバ400のFQDNは、DNS (Domain Name Server) などを用いて事前に取得するが、サーバ400のIPアドレス自体が既知の場合には、DNSは不要である。

[0160] 次に、図15のステップS702において、通信ノード300は、サーバ400との間でTCPセッションを開始するために、SYNパケットをサーバ400に送信する。送信パケットは、まず、通信ノード300にとってネットワーク600へのゲートウェイである、匿名化装置100に送られる。ここで、パケットを送信する際には、SYNパケットの宛先アドレスをSv__ADR1とし、送信元アドレスをCI__ADR1とし、宛先ポート番号を80とし、送信元ポート番号を20000とする。

[0161] 次に、図15のステップS703において、匿名化装置100は、SYNパケットを受信した場合に、図9に示した上述の一連の処理を実行する。ここで、匿名化装置100は、図9のステップS102における匿名化の要否判定では、匿名化ポリシーテーブル(図3)の検索の結果、発見したNo1のエントリの匿名化の要否の項目が'Yes'であるものとし、匿名化処理が必要であるものとする。そして、匿名化装置100は、図9のステップS103におけるセッションの開始判定では、受信したパケットがSYNパケット

であるため、セッション管理テーブル（図4）に、該当するセッションのエントリが存在するか否かを検索する。匿名化装置100は、検索の結果、該当するエントリが存在しないために、セッションの開始であるものと判定する。このため、図9のステップS104へと進む。

[0162] そして、匿名化装置100は、図9のステップS104では、図10に示したアルゴリズムに従って、プレフィクス情報テーブルから割当てプレフィクスを選択する。図5に示したプレフィクス情報テーブルの例では、Pref__A3と、Pref__B9とがプレフィクスの割当て候補となるが、ここでは、割当終了時刻が条件に合わなかったものと想定する。換言すると、図10のステップS205において条件を満足するプレフィクスが存在しない場合となり、図10のステップS202におけるプレフィクス割当要求処理を実施する。上述したように、図10のステップS202のプレフィクス割当要求処理の詳細は、図11に示したフローチャートを用いて示される。

[0163] 図11のステップS301において、匿名化装置100は、まず、プレフィクス割当要求信号を構成する。ここでは、プレフィクス割当要求信号には、要求プレフィクスセット数を1とし、既に保持しているプレフィクスセット情報を1とし、匿名化装置100のアドレスをCPE__ADR1として、それぞれの値が設定されるものと想定する。そして、匿名化装置100は、図11のステップS302においてプレフィクス割当要求信号をアンカーサーバ200に送信し、ステップS303においてプレフィクス割当応答信号の受信を待つ。

[0164] 次に、図15のステップS704において、アンカーサーバ200にプレフィクス割当要求信号が到達する。そして、ステップS705において、アンカーサーバ200は、図13に示したように、プレフィクス割当要求信号を受信した際の処理を実行する。ここでは、図13に示した処理の結果、貸出しプレフィクステーブル（図7）のプレフィクスセット番号2のプレフィクスセットが割当てられたものとする。プレフィクス割当処理の結果、アンカーサーバ200は、割当てたプレフィクスセット番号と、プレフィクスと

、I I D K e y と、失効時刻と、アンカーサーバ200のアドレスと、を格納したプレフィクス割当応答信号を、匿名化装置100に送信する。

[0165] 次に、図15のステップS706において、匿名化装置100にプレフィクス割当応答信号が到達する。そして、ステップS707において、匿名化装置100は、図11のステップS303におけるプレフィクス割当応答信号の受信待ち処理を抜け、ステップS304において、受信したプレフィクス割当応答信号に含まれるプレフィクス情報を用いて、プレフィクス情報テーブルを更新する。更新処理の結果、図16に示すように、プレフィクス情報テーブルに、プレフィクスセット番号2のエントリが追加される。

[0166] 次に、図10のステップS204において、匿名化装置100は、未使用プレフィクスの選択処理を行う。ここでは、P r e f _ A 4を選択するものとする。

[0167] 次に、図9のステップS105において、匿名化装置100は、上述した式1と式2を用いて求めたI I D部とプレフィクスP r e f _ A 4とを用いて、匿名アドレスを生成する。ここでは、生成した匿名アドレスをA n _ A D R 4とする。そして、匿名化装置100は、匿名アドレスを決定した後に、図9のステップS106において、セッション管理テーブルに新規のエントリを追加する。ここでは、図17に示すように、セッション管理テーブルにN o . 4のエントリが追加される。

[0168] 次に、図9のステップS110において、匿名化装置100は、セッション管理テーブルのN o . 4のエントリに基づいて、S Y Nパケットの送信元アドレスを、C I _ A D R 1からA n _ A D R 4に書き換えた後に、パケットをカプセル化して転送する。

[0169] 次に、図15のステップS708において、アンカーサーバ200は、カプセル化されたS Y Nパケットを匿名化装置100から受信した場合に、図14に示したフローチャートに従って、処理を実施する。ここで、アンカーサーバ200は、カプセル化されたS Y Nパケットを受信した時点では、匿名アドレス（A n _ A D R 4）のエントリが転送テーブルに存在しないため

に、新たなエントリを追加する。図 18 に、エントリが追加された転送テーブルを示す。ここでは、転送テーブルに追加されたエントリは No. 4 のエントリであるものとする。そして、アンカーサーバ 200 は、受信したパケットをデカプセル化した後に、サーバ 400 に転送する。

[0170] 次に、図 15 のステップ S709 において、サーバ 400 は、SYN パケットをアンカーサーバ 200 から受信した場合に、SYN+ACK パケットを匿名アドレス (An__ADR1) に応答する。An__ADR1 は、アンカーサーバ 200 に到達性のあるプレフィクス (Pref__A4) を有するため、SYN+ACK パケットは、アンカーサーバ 200 にルーティングされる。

[0171] 次に、アンカーサーバ 200 は、SYN+ACK パケットをサーバ 400 から受信した場合に、図 14 に示したフローチャートに従って、処理を実施する。ここでは、アンカーサーバ 200 は、転送テーブル (図 18) に No. 4 のエントリが存在するため、受信したパケットをカプセル化した後に、匿名化装置 100 のアドレス (CPE__ADR1) に転送する。

[0172] 次に、匿名化装置 100 は、カプセル化された SYN+ACK パケットを受信する。匿名化装置 100 のパケット処理手段 130 は、図 12 に示したフローチャートに従って、処理を実施する。パケット処理手段 130 は、セッション管理テーブル (図 17) に No. 4 のエントリが存在するため、受信したパケットをデカプセル化し、宛先アドレスを匿名アドレス (An__ADR1) から、通信ノード 300 のアドレス (CI__ADR1) に書き換える。そして、パケット処理手段 130 は、アドレスを書き換えたパケットを、通信ノード 300 に転送する。

[0173] 最後に、図 15 のステップ S710 において、通信ノード 300 とサーバ 400 との間で、ACK パケットやデータパケットがやり取りされる。上述した SYN パケットや SYN+ACK パケットと同様に、通信ノード 300 からサーバ 400 に送られるパケットは、匿名化装置 100 が匿名アドレスへの変換及びカプセル化を行い、さらに、アンカーサーバ 200 がデカプセ

ル化を行った後に、サーバ４００に到達する。また、サーバ４００から通信ノード３００に送られるパケットは、アンカーサーバ２００がカプセル化を行い、さらに、匿名化装置１００が、デカプセル化と、匿名アドレスを通信ノード３００のアドレスへと書き戻す処理と、を行う。

[0174] 以上説明したように、本実施の形態１に係る通信システム１は、匿名化装置１００において、セッション管理手段１２２がセッションを識別し、匿名アドレス選択手段１２３と匿名アドレス１２４がセッション単位で異なる匿名アドレスを生成し、さらに、パケット処理手段１３０が通信ノード３００の送信パケットの送信元アドレスを匿名アドレスに書き換えた上で、匿名アドレスを用いて到達性のあるアンカーサーバ２００にトンネリングする構成とした。

[0175] これにより、セッション単位で個別の匿名アドレスを設定することができ、さらに、匿名アドレスについてプレフィクス部も含めた匿名性を確保することができる。また、匿名アドレスは匿名化装置１００のインタフェースに割当てて必要が無いため、Neighbor Cacheの負荷の問題も発生せず、DADを用いた処理の遅延の問題も発生しない。また、上述した特許文献１におけるイングレスフィルタの問題や、TCPに適用できないという問題も発生しない。また、一般的なIPノードである移動ノード３００に対しても、匿名アドレスを用いた通信環境を提供することができる。

[0176] また、本実施の形態１に係る通信システム１では、匿名アドレス選択手段１２３がプレフィクスを選択する際に、その選択以前にプレフィクスを選択した時刻を考慮する構成としたことで、近い時間内に同じプレフィクスを有する匿名アドレスの使用を回避することができ、高い匿名性を実現できる。

[0177] また、本実施の形態１に係る通信システム１は、匿名アドレスを構成する際に候補となるプレフィクスが無かった場合には、匿名アドレス選択手段１２３がプレフィクス割当要求信号を送信することで、アンカーサーバ２００にプレフィクスの割当を要求する。ここで、プレフィクスの割当を要求する際には、匿名化装置１００が既に保持しているプレフィクス情報を渡す構成

としたことで、アンカーサーバ200は匿名化装置100に割当てたプレフィクス情報を保持しておく必要がなく、匿名化装置100が未だに保持していないプレフィクスを割当てることができる。

[0178] さらに、プレフィクスの割当を要求する際には、匿名化装置100が既に保持しているプレフィクスを、プレフィクスセット番号を用いて通知する構成としたことで、プレフィクス割当要求信号のサイズを小さくすることができる。また、匿名化装置100が未だ保持していないプレフィクスについて、アンカーサーバ200が行う検索処理の処理量を小さくすることができる。この特徴は、例えば、膨大な数の匿名化装置100に対して匿名化サービスを提供する場合に、非常に有効な特徴となる。

[0179] また、本実施の形態1に係る通信システム1では、匿名アドレス生成手段124が、匿名アドレスやポート番号といったサーバ400の管理者が取得し得る情報と、アンカーサーバ200を管理するオペレータのみが保持する情報と、を使用して、匿名アドレスを使用した匿名化装置100を特定可能とするように、匿名アドレスを算出する。これにより、アンカーサーバ200を管理するオペレータは、セッション毎に変化する匿名アドレスと匿名化装置100との対応関係を逐次記録する必要がなく、追跡性を確保することができる。

[0180] 実施の形態2.

次に、図19乃至26を参照して、本発明の実施の形態2について説明する。

(構成の説明)

まず、図19乃至図23を参照して、本実施の形態2に係る通信システム1の構成について説明する。本実施の形態2に係る通信システム1の全体構成は、図1に示した実施の形態1に係る通信システム1と略同様の構成である。本実施の形態2に係る通信システム1では、図2で示した匿名化装置100が図19に示す匿名化装置101となり、図6で示したアンカーサーバ200が図20に示すアンカーサーバ201となる点で異なる。また、本実

施の形態 2 に係る通信システム 1 では、匿名化装置 101 ではなく、アンカーサーバ 201 が匿名化アドレスへの書き換えを行うように構成されている点で異なる。

[0181] 図 19 は、匿名化装置 101 を示す構成図である。図に示すように、匿名化装置 101 は、インタフェース 110A と、インタフェース 110B と、匿名化制御手段 120__2 と、パケット処理手段 130__2 と、情報記録装置 140 と、を備えている。匿名化制御手段 120__2 は、匿名性確保要否判定手段 121 と、セッション管理手段 122__2 と、アンカー選択手段 125 と、を備えている。尚、図 2 に示した匿名化装置 100 の各要素と同一の機能を有する要素は、図 19 において同一の名称及び符号を用いて示すものとし、以下では、その詳細な説明を省略する。

[0182] セッション管理手段 122__2 は、実施の形態 1 に係るセッション管理手段 122 と同様に、通信の特定の一連の単位であるセッションの開始及び終了を判定する機能と、情報記録装置 140 に記録されたセッション管理テーブルを管理する機能と、を備えている。尚、図 21 に示すように、セッション管理手段 122__2 が管理するセッション管理テーブルは、匿名アドレスを含まない点において、実施の形態 1 に係るセッション管理テーブルと異なる。

[0183] また、セッション管理手段 122__2 は、匿名アドレスの割当て要求に代えて、匿名化処理を依頼するアンカーサーバ 201 の割当て要求を、アンカー選択手段 125 に出力する。セッション管理手段 122__2 は、アンカーサーバ 201 の割当て要求の結果、アンカーサーバ 201 のアドレスを取得した場合には、取得したアンカーサーバ 201 のアドレスを、セッション管理テーブル（図 21）のアンカーサーバアドレスの項目に設定する。

[0184] アンカー選択手段 125 は、セッション管理手段 122__2 からのアンカーサーバ割当て要求に応じて、匿名化処理を依頼するアンカーサーバ 201 を選択し、選択したアンカーサーバ 201 のアドレスをセッション管理手段 122__2 に応答する機能を備えている。アンカー選択手段 125 は、匿名化

装置 101 に事前に設定されたアンカーサーバ 201 のアドレスから、アンカーサーバ 201 のアドレスをランダムに選択する。

[0185] 尚、アンカー選択手段 125 が、通信ノード 300 から送信されたパケットの宛先アドレスを取得できるようにし、かつ、割当てたアンカーサーバ 201 と、送信されたパケットの宛先アドレスと、受信時刻と、を関連付けて記録しておくようにした上で、宛先アドレスが同じセッションに対しては、所定の時間内に割当てたアンカーサーバ 201 と同じアドレスを選択しない、或いは、選択確率に重み付けをすることで同じアドレスを選択しにくくするものとしても良い。勿論、他の選択方法を用いて選択するものとしても良い。

[0186] パケット処理手段 130__2 は、実施の形態 1 に係るパケット処理手段 130 と同様に、情報記録装置 140 に記録されたセッション管理テーブルを参照して、パケットのカプセル化及びデカプセル化を実施する。尚、パケット処理手段 130__2 は、通信ノード 300 のアドレスから匿名アドレスへの書換えと、匿名アドレスから通信ノード 300 のアドレスへの書換えと、を行わない点において、実施の形態 1 に係るパケット処理手段 130 と異なる。

[0187] 情報記録装置 140 は、図 3 に示したポリシテーブルと、図 21 に示したセッション管理テーブルと、を記録する記録装置である。

[0188] 図 20 は、アンカーサーバ 201 を示す構成図である。図に示すように、アンカーサーバ 201 は、インタフェース 210 と、匿名化装置判定手段 260 と、匿名化制御手段 270 と、パケット処理手段 280 と、情報記録装置 290 と、を備えている。尚、図 6 に示したアンカーサーバ 200 の各要素と同一の機能を有する要素は、図 20 において同一の名称及び符号を用いて示すものとし、以下では、その詳細な説明を省略する。

[0189] 匿名化装置判定手段 260 は、インタフェース 210 が受信したパケットがカプセル化されたパケットである場合には、外側 IP ヘッダの宛先アドレスがアンカーサーバ 201 のアドレスであり、かつ、外側 IP ヘッダの送信

元アドレスがアンカーサーバ201の使用を許可した匿名化装置101であるか否かを確認する。匿名化装置判定手段260は、確認の結果、条件に適合したパケットを匿名化制御手段270に出力する。匿名化装置判定手段260は、条件に適合しなかったパケットは、破棄する。尚、パケットを破棄せずに、一般的なルーティング処理を単に実施するものとしても良い。

[0190] ここで、匿名化装置判定手段260が、匿名化装置101がアンカーサーバ201の使用を許可されているか否かの判定を行うに際しては、許可する匿名化装置101のアドレスのリストを事前に保持しておき、保持したリストを判定時に参照すれば良い。また、例えば、トンネル化されたパケットに、アンカーサーバ201の使用を許可されている旨の証明情報を付与する方法を適用するなど、他の方法を適用しても良い。

[0191] 匿名化制御手段270は、匿名化装置判定手段260からパケットが入力された場合に、入力されたパケットの情報や、情報記録装置290に記録されたプレフィクス情報テーブルの情報（図22）などを使用して、匿名アドレスを生成する。また、匿名化制御手段270は、通信ノード300のアドレスを匿名アドレスへと書き換えるための準備を行う。さらに、匿名化制御手段270は、入力されたパケットを、パケット処理手段280に出力する。

[0192] 図20に示すように、匿名化制御手段270は、セッション管理手段271と、匿名アドレス選択手段272と、匿名アドレス生成手段273と、を備えている。匿名化制御手段270は、実施の形態1に係る匿名化制御手段120と類似する機能を備えている。

[0193] セッション管理手段271は、実施の形態1に係るセッション管理手段122と同様に、匿名化装置判定手段260からパケットが入力された場合に、セッションの開始及び終了を判定する機能と、情報記録装置290に記録されたセッション管理テーブルを管理する機能と、を備えている。本実施の形態2では、セッションとしてTCPセッションを想定しており、TCPセッションは宛先アドレスと、送信元アドレスと、宛先ポート番号と、送信元

ポート番号と、に基づいて識別される。尚、TCPセッションに限定されず、他の単位をセッションとみなしても良い。

[0194] セッション管理手段271が有する機能（即ち、セッションの開始及び終了を判定する機能と、セッションを管理する機能）は、実施の形態1に係るセッション管理手段122が有する機能と略同じであるが、カプセル化されたパケットの内側に格納されたIPパケットを使用して、セッションの開始及び終了を判定する点において異なる。

[0195] また、セッション管理手段271が管理するセッション管理テーブルは、図22に示したように、アンカーサーバ201のアドレスに代えて、匿名化装置101のアドレスを記録する点において異なる。

[0196] セッション管理手段271は、新規セッション用のエントリの作成時には、カプセル化されたパケットの外側IPヘッダの送信元アドレスを、匿名化装置101のアドレスの項目に設定することができる。或いは、匿名化装置判定手段260が、アンカーサーバ201の使用が認められた匿名化装置101であると判定した後に、匿名化装置101のアドレスをセッション管理手段271に別途出力する構成とすることで、セッション管理手段271は、入力された匿名化装置101のアドレスを、セッション管理テーブルの匿名化装置アドレスの項目に設定しても良い。

[0197] さらに、セッション管理手段271は、エントリを追加する際には、匿名アドレス選択手段272に匿名アドレスを要求して、要求の結果得られた匿名アドレスを、セッション管理テーブルの匿名アドレスの項目に設定する。

[0198] 匿名アドレス選択手段272は、セッション管理手段271から匿名アドレスを要求された場合に、情報記録装置290に記録されたプレフィクス情報テーブル（図23）から1つのプレフィクスをランダムで選択する。尚、プレフィクスの選択方法としては、プレフィクスと、プレフィクスを割当てた匿名化装置101と、割当時刻と、を対応づけて記録しておき、同じ匿名化装置101に対しては所定の時間内に同一のプレフィクスを選択しない、或いは、選択確率に重み付けをすることで同一のプレフィクスを選択しにく

くするものとしても良い。

- [0199] 匿名アドレス選択手段272は、プレフィクスを選択した後、選択したプレフィクスとプレフィクスに対応づけられたIID Key情報とを匿名アドレス生成手段273に出力することで、匿名アドレスを取得する。そして、匿名アドレス選択手段272は、取得した匿名アドレスを、セッション管理手段271に応答する。
- [0200] 匿名アドレス生成手段273は、実施の形態1に係る匿名アドレス生成手段124と同様の動作をするため、ここではその詳細な説明を省略する。
- [0201] パケット処理手段280は、情報記録装置290に記録されたセッション管理テーブルを参照することで、パケット処理手段280に入力されたパケットに対して、デカプセル化を行った後に、送信元アドレスを匿名アドレスに書き換える処理を行う。また、パケット処理手段280は、セッション管理テーブルを参照することで、パケット処理手段280に入力されたパケットに対して、通信ノード300のアドレスに匿名アドレスを書き換えた後に、カプセル化する処理を実施する。さらに、パケット処理手段280は、デカプセル化或いはカプセル化したパケットを、一般的なIPルーティングの処理を用いて、転送を行う。
- [0202] また、パケット処理手段280は、カプセル化されたパケットに対してセッション管理テーブルの検索を行う場合には、外側IPヘッダの送信元アドレスと、内側IPヘッダの宛先アドレスと、内側IPヘッダの送信元アドレスと、宛先ポート番号と、送信元ポート番号と、を、セッション管理テーブルの匿名化装置アドレスと、宛先アドレスと、送信元アドレスと、宛先ポートと、送信元ポートと、それぞれ設定された値と比較する。比較の際には、パケット処理手段280は、外側IPヘッダの宛先アドレスがアンカーサーバ201のアドレスと一致しているか否かについても確認する。
- [0203] 一方で、パケット処理手段280は、カプセル化されていないパケットの受信時にセッション管理テーブルを検索する場合には、受信パケットの宛先アドレスと、セッション管理テーブルの匿名アドレスに設定されたアドレス

と、を比較する。比較の結果、適合するエントリを発見した場合には、パケット処理手段 280 は、受信パケットの宛先アドレスを、セッション管理テーブルの送信元アドレスに設定されたアドレスに書き換える。そして、パケット処理手段 280 は、セッション管理テーブルの匿名化装置アドレスに設定されたアドレスを外側 IP ヘッダの宛先アドレスとし、また、アンカーサーバ 201 のアドレスを外側 IP ヘッダの送信元アドレスとして、カプセル化を行う。

- [0204] 情報記録装置 290 は、図 22 に示したセッション管理テーブルと、図 23 に示したプレフィクス情報テーブルとを記録する記録装置である。
- [0205] 上記した、匿名化制御手段 120__2 と、パケット処理手段 130__2 と、匿名化装置判定手段 260 と、匿名化制御手段 270 と、パケット処理手段 280 と、は、いずれもソフトウェアを用いてその機能を実現することができる。さらに、これら手段のいずれか一部或いは全てを、ハードウェアを用いて構成することも可能である。
- [0206] また、上述した情報記録装置 290 は、情報を記録可能な装置（半導体メモリやハードディスクドライブなど）を用いて構成することができる。
- [0207] 尚、図 19 乃至図 23 に示した各手段や装置の構成は例示にすぎず、本発明の趣旨を逸脱しない範囲で他の構成を用いて実現するものとしても良い。
- [0208] 実施の形態 2 に係る通信システム 1 の構成によれば、アンカーサーバ 201 が匿名アドレスへの書換え処理を実施することで、匿名化装置 101 が行う処理を簡略化することができる。
- [0209] また、匿名性を多少弱める方向としても構わないのであれば、匿名化装置 101 とアンカーサーバ 201 との間に、静的なトンネルを張る構成としても良い。かかる構成によれば、匿名化装置 101 の匿名化制御手段 120__2 が不要となり、匿名化装置 101 が行う処理をより簡略化することができる。尚、情報記録装置 140 のセッション管理テーブルに、事前に 1 つのエントリを例えば手動で作成することで、静的なトンネルを張ることができる。

[0210] (動作の説明)

次に、図 2 4 乃至図 2 6 を参照して、本実施の形態 2 に係る通信システム 1 の動作について説明する。図 2 4 は、通信ノード 3 0 0 からパケットを受信した場合の、匿名化装置 1 0 1 の動作を示すフローチャートである。図 2 5 及び図 2 6 は、アンカーサーバ 2 0 1 の動作を示すフローチャートである。

[0211] 図 2 4 において、まず始めに、匿名化装置 1 0 1 の匿名化制御手段 1 2 0 __2 は、通信ノード 3 0 0 が送信したパケットを、インタフェース 1 1 0 A を介して受信する（ステップ S 8 0 1）。そして、匿名性確保要否判定手段 1 2 1 は、受信パケットに対して匿名性を確保する必要があるか否かを判定する（ステップ S 8 0 2）。ここで、匿名性が必要と判定された場合（即ち、' Y ' の場合）には、ステップ S 8 0 3 へと進む。一方で、匿名性が不必要と判定された場合（即ち、' N ' の場合）には、ステップ S 8 0 9 へと進む。

[0212] 次に、セッション管理手段 1 2 2 __2 は、ステップ S 8 0 2 で匿名性が必要と判定した場合には、受信パケットの内容をチェックし、セッションの開始であるか否かを判定する（ステップ S 8 0 3）。尚、セッションの開始判定方法については上述した内容と同一であるため、ここではその説明を省略する。ここで、セッションの開始であると判定された場合（即ち、' Y ' の場合）には、ステップ S 8 0 4 へと進む。セッションの開始でないと判定された場合（即ち、' N ' の場合）には、ステップ S 8 0 6 へと進む。

[0213] 次に、アンカー選択手段 1 2 5 は、ステップ S 8 0 3 でセッションの開始であると判定した場合には、匿名アドレスへのアドレス書換えを依頼するアンカーサーバ 2 0 1 を選択する（ステップ S 8 0 4）。

[0214] 次に、セッション管理手段 1 2 2 __2 は、アンカー選択手段 1 2 5 が選択したアンカーサーバ 2 0 0 のアドレスと、ステップ S 8 0 1 における受信パケットから取得したセッションを識別するための情報と、を用いて、セッション管理テーブルに新規のエントリを作成する（ステップ S 8 0 5）。ステ

ップS 8 0 5での処理が終了した後、ステップS 8 0 9へと進む。

[0215] また、セッション管理手段1 2 2__2は、ステップS 8 0 3でセッションの開始でないと判定された場合には、セッションの終了判定を行う（ステップS 8 0 6）。尚、セッションの終了判定方法については上述した内容と同一であるため、ここではその説明を省略する。ここで、セッションの終了であると判定された場合（即ち、' Y' の場合）には、ステップS 8 0 7へと進む。セッションの終了でないと判定された場合（即ち、' N' の場合）には、ステップS 8 0 8へと進む。

[0216] 次に、セッション管理手段1 2 2__2は、ステップS 8 0 6でセッションの終了であると判定した場合には、セッション終了時の処理を行う（ステップS 8 0 7）。具体的には、セッション管理手段1 2 2__2は、セッション管理テーブルから対応するエントリを削除する。ステップS 8 0 7での処理が終了した後、ステップS 8 0 9へと進む。

[0217] また、セッション管理手段1 2 2__2は、ステップS 8 0 6でセッションの終了でないと判定した場合には、セッション管理テーブルの失効時刻を更新する（ステップS 8 0 8）。ステップS 8 0 8での処理が終了した後、ステップS 8 0 9へと進む。

[0218] 最後に、パケット処理手段1 3 0__2は、セッション管理テーブルの情報を参照して、セッション管理テーブルの対応するエントリに設定されたアンカーサーバ2 0 1のアドレスへとトンネリングするための、カプセル化処理を行う（ステップS 8 0 9）。

[0219] 次に、図2 5及び図2 6を参照して、アンカーサーバ2 0 1の動作について詳細に説明する。図2 5は、匿名化装置1 0 1から送信された（カプセル化された）パケットを受信した場合の、アンカーサーバ2 0 1の動作を示すフローチャートである。

[0220] 図2 5において、まず始めに、アンカーサーバ2 0 1の匿名化装置判定手段2 6 0は、匿名化装置1 0 1が送信したパケットを、インタフェース2 1 0を介して受信する（ステップS 9 0 1）。そして、匿名化装置判定手段2

60は、受信したパケットが、アンカーサーバ201の使用が許可された匿名化装置101から送信されたパケットであるか否かを判定する（ステップS902）。尚、受信パケットの判定方法については上述した内容と同一であるため、ここではその説明を省略する。ここで、受信パケットが、許可された匿名化装置101から受信したパケットであると判定された場合（即ち、'Y'の場合）には、ステップS903へと進む。一方で、受信パケットが、許可された匿名化装置101から受信したパケットでないと判定された場合（即ち、'N'の場合）には、ステップS910へと進む。

[0221] 次に、セッション管理手段271は、ステップS902で許可された匿名化装置101から受信したパケットであると判定した場合には、受信パケットの内容をチェックし、セッションの開始であるか否かを判定する（ステップS903）。ここで、セッションの開始であると判定された場合（即ち、'Y'の場合）には、ステップS904へと進む。セッションの開始でないと判定された場合（即ち、'N'の場合）には、ステップS907へと進む。

[0222] 次に、匿名アドレス選択手段272は、ステップS904でセッションの開始であると判定された場合には、情報記録装置290に記録されたプレフィクス情報テーブル（図23）の情報から、匿名アドレスを生成する際に使用するプレフィクスを選択する（ステップS904）。

[0223] 次に、匿名アドレス生成手段273は、選択したプレフィクスと、プレフィクスに関連づけられたIID Keyと、を使用して、匿名アドレスを生成する（ステップS905）。尚、匿名アドレスの生成方法については上述した内容と同一であるため、ここではその説明を省略する。

[0224] 次に、セッション管理手段271は、匿名アドレスと、ステップS901における受信パケットから取得したセッションを識別するための情報と、パケットを送信してきた匿名化装置101のアドレスと、を用いて、セッション管理テーブルに新規なエントリを作成する（ステップS906）。ステップS906での処理が終了した後、ステップS910へと進む。

[0225] また、セッション管理手段271は、ステップS903でセッションの開

始でないと判定した場合には、セッションの終了判定を行う（ステップS 9 0 7）。ここで、セッションの終了であると判定された場合（即ち、' Y ' の場合）には、ステップS 9 0 8へと進む。一方で、セッションの終了でないと判定された場合（即ち、' N ' の場合）には、ステップS 9 0 9へと進む。

[0226] 次に、セッション管理手段2 7 1は、ステップS 9 0 3でセッションの終了であると判定した場合には、セッション終了時の処理を行う（ステップS 9 0 8）。具体的には、セッション管理手段2 7 1は、セッション管理テーブルから対応するエントリを削除する。ステップS 9 0 8での処理が終了した後、ステップS 9 1 0へと進む。

[0227] また、セッション管理手段2 7 1は、ステップS 9 0 7でセッションの終了でないと判定した場合には、セッション管理テーブルの失効時刻を更新する（ステップS 9 0 9）。ステップS 9 0 9での処理が終了した後、ステップS 9 1 0へと進む。

[0228] 最後に、パケット処理手段2 8 0は、匿名化装置1 0 1から送信された（カプセル化された）パケットについて、デカプセル化処理を行い、さらに、送信元アドレスを匿名アドレスに書き換えた後に、宛先アドレスへと転送する（ステップS 9 1 0）。尚、パケット処理手段2 8 0が行うステップS 9 1 0での処理の詳細については、図2 6を参照して後述する。

[0229] 次に、図2 6を参照して、図2 5のステップS 9 1 0における処理の詳細について説明する。図2 6は、アンカーサーバ2 0 1のパケット処理手段2 8 0が行う処理の動作を示すフローチャートである。尚、パケット処理は、匿名化装置1 0 1から送信された（カプセル化された）パケットであって、匿名化制御手段2 7 0が処理した後のパケットや、インタフェース2 1 0が受信した匿名化アドレス宛のパケットに対して行われる処理を示す。匿名化装置1 0 1から送信された（カプセル化された）パケットであって、匿名化制御手段2 7 0が処理した後のパケットに対して行われる処理が、図2 5のステップS 9 1 0で行われるパケット処理に相当する。

[0230] 図2 6において、まず、アンカーサーバ2 0 1のパケット処理手段2 8 0

は、受信したパケットがカプセル化されているか否かを判定する（ステップ S 1 0 0 1）。ここで、受信パケットがカプセル化されていると判定された場合（即ち、'Y' の場合）には、ステップ S 1 0 0 2 へと進む。一方で、受信パケットがカプセル化されていないと判定された場合（即ち、'N' の場合）には、ステップ S 1 0 0 6 へと進む。

[0231] 次に、パケット処理手段 2 8 0 は、ステップ S 1 0 0 1 で受信パケットがカプセル化されていないと判定した場合には、受信したパケットに設定された情報を使用して、情報記録装置 2 9 0 に記録されたセッション管理テーブルを検索し（ステップ S 1 0 0 2）、対応するエントリが存在するか否かを確認する（ステップ S 1 0 0 3）。尚、ステップ S 1 0 0 2 で検索を行う際に比較される情報は、上述したパケット処理手段 2 8 0 の説明において既に述べたため、ここではその説明を省略する。ステップ S 1 0 0 3 での確認の結果、対応するエントリが発見された場合（即ち、'Y' の場合）には、ステップ S 1 0 0 4 へと進む。一方で、発見されなかった場合（即ち、'N' の場合）には、ステップ S 1 0 1 0 へと進む。

[0232] 次に、パケット処理手段 2 8 0 は、ステップ S 1 0 0 3 で対応するエントリを発見した場合には、受信したパケットの宛先アドレスを、匿名アドレスから、発見したエントリの送信元アドレスに書き換える（ステップ S 1 0 0 4）。

[0233] 次に、パケット処理手段 2 8 0 は、ステップ S 1 0 0 4 で宛先アドレスを書き換えたパケットについて、匿名化装置 1 0 1 に転送するためのカプセル化処理を行う（ステップ S 1 0 0 5）。ステップ S 1 0 0 5 での処理が終了した後、ステップ S 1 0 1 0 へと進む。

[0234] 一方で、パケット処理手段 2 8 0 は、ステップ S 1 0 0 1 で受信パケットがカプセル化されていると判定した場合には、受信したパケット（カプセル化されたパケット）に設定された情報を使用して、情報記録装置 2 9 0 に記録されたセッション管理テーブルを検索し（ステップ S 1 0 0 6）、対応するエントリが存在するか否かを確認する（ステップ S 1 0 0 7）。尚、ステ

ステップS1006で検索を行う際に比較される情報は、上述したパケット処理手段280の説明において既に述べたため、ここではその説明を省略する。ステップS1007での確認の結果、対応するエントリが発見された場合（即ち、'Y'の場合）には、ステップS1008へと進む。一方で、発見されなかった場合（即ち、'N'の場合）には、ステップS1010へと進む。

[0235] 次に、パケット処理手段280は、ステップS1007で対応するエントリが発見された場合には、受信したパケットについて、デカプセル化を行う（ステップS1008）。具体的には、パケット処理手段280は、受信したパケットの外側IPヘッダを除去する。

[0236] 次に、パケット処理手段280は、デカプセル化後のパケットの送信元アドレスを、セッション管理テーブルの匿名アドレスに記録されたアドレスに書換える（ステップS1009）。ステップS1009での処理が終了した後、ステップS1010へと進む。

[0237] 最後に、パケット処理手段280は、通常のIPルーティングの機能を用いてパケットをルーティングして、インタフェース210からネットワーク600へと送出する（ステップS1010）。

[0238] 以下、本発明に係る通信システムに基づく効果を説明する。

第1の効果は、一般的なIPノードである通信ノードに対して、高い匿名性を確保した通信を提供できることである。その理由は、通信ノードが送信したパケットの送信元アドレス（即ち、通信ノードのアドレス）を匿名化装置が匿名アドレスに書き換え、さらに、匿名アドレスのプレフィクスを用いて到達性のあるアンカーサーバにトンネリングする構成としたことで、プレフィクス部も含めたアドレス全体を、匿名性が確保されたアドレスに書換える可能としたためである。また、セッション単位で、異なる匿名アドレスを使用できる構成としたためである。

[0239] 第2の効果は、匿名化装置との間で非公開の情報（即ち、IID_Key）を共有することで、匿名アドレスと通信ノードのアドレスとの対応関係を逐次記録する必要がなく、匿名アドレスを使用した匿名化装置を匿名アドレ

スから特定可能な追跡機能を提供できることである。その理由は、匿名アドレス生成手段において、非公開の情報を使用して、匿名化装置を特定できる情報に変換可能となるように、匿名アドレスの一部（IID部）を生成する構成としたためである。

[0240] また、本発明に係る通信システムは、IPv6を用いた通信システムに対して広く適用可能である。例えば、本発明に係るアンカーサーバをISP（Internet Service Provider）に配備すると共に、本発明に係る匿名化装置の機能を、ISPの加入者であるユーザ宅に置かれるブロードバンドルータなどのCPE（Customer Premises Equipment）において実施することが可能である。これにより、ISPは、ユーザに対して、匿名性の確保された通信を提供することができる。

[0241] さらに、本発明に係る通信システムによれば、ISP以外のサーバが匿名アドレスを使用した不正アクセスを受けた場合には、ISP以外のサーバの管理者により、不正アクセス時の匿名アドレスとポート番号とが記録されたログをISPに通知してもらうことで、ISPは、匿名アドレスを元に、不正アクセスを行ったユーザを特定することができるため、匿名性に起因する悪影響を抑制することができる。従って、匿名性の提供と、必要な場合には追跡性の確保とを両立させることができるため、ISPのサービスなどについて、本発明に係る通信システムの適用は非常に有効なものとなる。

[0242] 尚、本発明は上記実施の形態に限られたものではなく、趣旨を逸脱しない範囲で適宜変更することが可能である。

[0243] この出願は、2009年3月6日に提出された日本出願特願2009-052919を基礎とする優先権を主張し、その開示の全てをここに取り込む。

符号の説明

[0244] 100、101 匿名化装置、
200、201 アンカーサーバ、
300 通信ノード、

4 0 0 サーバ、
5 0 0 ローカルネットワーク、
6 0 0 ネットワーク、
1 1 0 A、1 1 0 B インタフェース、
1 2 0、1 2 0__2 匿名化制御手段、
1 2 1 匿名性確保要否判定手段、
1 2 2、1 2 2__2 セッション管理手段、
1 2 3 匿名アドレス選択手段、
1 2 4 匿名アドレス生成手段、
1 3 0、1 3 0__2 パケット処理手段、
1 4 0 情報記録装置、
2 1 0 インタフェース、
2 2 0 プレフィクス割当手段、
2 3 0 転送手段、
2 4 0 プレフィクス記録装置、
2 5 0 転送情報記録装置、
2 6 0 匿名化装置判定手段、
2 7 0 匿名化制御手段、
2 7 1 セッション管理手段、
2 7 2 匿名アドレス選択手段、
2 7 3 匿名アドレス生成手段、
2 8 0 パケット処理手段、
2 9 0 情報記録装置、
p 1 0 発信側情報処理装置、
p 2 0 仮アドレスサーバ、
p 3 0 受信側情報処理装置、
p 4 0 インターネット

請求の範囲

[請求項1]

通信ノードと第1のネットワークを介して接続される匿名化装置と、当該匿名化装置と第2のネットワークを介して接続されるサーバと、を有し、

前記匿名化装置は、

前記サーバから取得したプレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、

前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットの送信元アドレスを前記匿名アドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備え、

前記サーバは、

前記匿名化装置から送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第2のネットワークに送出する転送手段を備える

ことを特徴とする通信システム。

[請求項2]

前記サーバの前記転送手段は、

送信先アドレスが前記匿名アドレスであるパケットを受信した場合に、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記サーバのアドレスとし、かつ、送信先アドレスを前記匿名化装置のアドレスとして当該カプセル化パケットを前記第2のネットワークに送出し、

前記匿名装置の前記パケット処理手段は、

前記サーバから送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信先アドレスを前記通信ノードのアドレスとして前記第1

のネットワークに送出する

ことを特徴とする請求項 1 に記載の通信システム。

[請求項3]

前記匿名化装置は、

前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットのセッションを識別し、当該識別したセッションと前記匿名アドレスとを対応付けて管理するセッション管理手段を更に備え、

前記匿名化装置の前記匿名アドレス生成手段は、

前記サーバから取得したプレフィクスと、前記セッション毎に変化させるインタフェース ID と、に基づいて、匿名アドレスを生成する

ことを特徴とする請求項 1 に記載の通信システム。

[請求項4]

前記匿名化装置は、

複数の前記プレフィクスから一のプレフィクスを選択する匿名アドレス選択手段を更に備える

ことを特徴とする請求項 1 に記載の通信システム。

[請求項5]

前記匿名化装置の前記匿名アドレス選択手段は、

複数の前記プレフィクスから一のプレフィクスを選択する場合に、当該選択よりも前の所定の時間内に選択したプレフィクスとは異なるプレフィクスを選択する

ことを特徴とする請求項 4 に記載の通信システム。

[請求項6]

前記匿名化装置の前記匿名アドレス選択手段は、

複数の前記プレフィクスから一のプレフィクスを選択するときに、前記匿名アドレスの生成に未だに割当てられていないプレフィクスが存在しない場合には、前記サーバに対してプレフィクス割当要求信号を送信し、

前記サーバは、

前記匿名化装置から送信された前記プレフィクス割当要求信号を受信した場合には、前記匿名化装置にプレフィクスを割当て、当該割当てたプレフィクス情報を含むプレフィクス割当応答信号を前記匿名化

装置に送信するプレフィクス割当手段を更に備える

ことを特徴とする請求項 4 に記載の通信システム。

[請求項7]

前記プレフィクス割当要求信号は、

前記サーバから取得した複数のプレフィクスからなるプレフィクス群であって、当該プレフィクス群に割当てられたプレフィクスセット番号を含む

ことを特徴とする請求項 6 に記載の通信システム。

[請求項8]

前記匿名化装置の前記匿名アドレス生成手段は、

前記通信ノードから送信されたパケットを受信した場合に、

前記サーバから取得した第 1 のインタフェース ID 生成用情報と、前記匿名化装置の識別子と、に基づいて、インタフェース ID を作成し、前記サーバから取得したプレフィクスと前記作成したインタフェース ID とから前記匿名アドレスを生成する

ことを特徴とする請求項 1 に記載の通信システム。

[請求項9]

前記匿名化装置の前記匿名アドレス生成手段は、

前記通信ノードから送信されたパケットを受信した場合に、

前記サーバから取得した第 1 のインタフェース ID 生成用情報と、前記通信ノードから送信されたパケットの送信元ポート番号と、に基づいて第 2 のインタフェース ID 生成用情報を生成し、当該生成した第 2 のインタフェース ID 生成用情報と、前記匿名化装置の識別子と、に基づいて、前記インタフェース ID を作成する

ことを特徴とする請求項 8 に記載の通信システム。

[請求項10]

前記匿名化装置は、

前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットに対して匿名性を確保する必要があるか否かを判定する匿名性確保要否判定手段を更に備える

ことを特徴とする請求項 1 に記載の通信システム。

[請求項11]

通信ノードと第 1 のネットワークを介して接続される匿名化装置と

、当該匿名化装置と第2のネットワークを介して接続されるサーバと、を有し、

前記匿名化装置は、

前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備え、

前記サーバは、

プレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、

前記匿名化装置から送信されたカプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信元アドレスを前記匿名アドレスに書き換えた後に、当該デカプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備える

ことを特徴とする通信システム。

[請求項12]

前記サーバの前記パケット処理手段は、

送信先アドレスが前記匿名アドレスであるパケットを受信した場合に、当該受信パケットの送信先アドレスを前記通信ノードのアドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記サーバのアドレスとし、かつ、送信先アドレスを前記匿名化装置のアドレスとして当該カプセル化パケットを前記第2のネットワークに送出し、

前記匿名装置の前記パケット処理手段は、

前記サーバから送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第1のネットワ

ークに送出する

ことを特徴とする請求項 11 に記載の通信システム。

[請求項13]

前記サーバは、

前記匿名化装置から送信されたカプセル化パケットを受信した場合に、当該受信パケットのセッションを識別し、当該識別したセッションと前記匿名アドレスとを対応付けて管理するセッション管理手段を更に備え、

前記サーバの前記匿名アドレス生成手段は、

前記プレフィクスと、前記セッション毎に変化させるインタフェース ID と、に基づいて、匿名アドレスを生成する

ことを特徴とする請求項 11 に記載の通信システム。

[請求項14]

前記サーバは、

複数の前記プレフィクスから一のプレフィクスを選択する匿名アドレス選択手段を更に備える

ことを特徴とする請求項 11 に記載の通信システム。

[請求項15]

前記サーバの前記匿名アドレス選択手段は、

複数の前記プレフィクスから一のプレフィクスを選択する場合に、当該選択よりも前の所定の時間内に選択したプレフィクスとは異なるプレフィクスを選択する

ことを特徴とする請求項 14 に記載の通信システム。

[請求項16]

前記サーバの前記匿名アドレス生成手段は、

前記匿名化装置から送信されたカプセル化パケットを受信した場合に、

第 1 のインタフェース ID 生成用情報と、前記匿名化装置の識別子と、に基づいて、インタフェース ID を作成し、前記サーバから取得したプレフィクスと前記作成したインタフェース ID とから前記匿名アドレスを生成する

ことを特徴とする請求項 11 に記載の通信システム。

- [請求項17] 前記サーバの前記匿名アドレス生成手段は、
前記匿名化装置から送信されたカプセル化パケットを受信した場合に、
前記第1のインタフェースID生成用情報と、前記匿名化装置から送信されたパケットの送信元ポート番号と、に基づいて第2のインタフェースID生成用情報を生成し、当該生成した第2のインタフェースID生成用情報と、前記匿名化装置の識別子と、に基づいて、前記インタフェースIDを作成する
ことを特徴とする請求項16に記載の通信システム。
- [請求項18] 前記匿名化装置は、
前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットに対して匿名性を確保する必要があるか否かを判定する匿名性確保要否判定手段を更に備える
ことを特徴とする請求項11に記載の通信システム。
- [請求項19] 匿名化装置は、
第1のネットワークを介して接続された通信ノードから送信されたパケットを受信した場合に、
前記匿名化装置と第2のネットワークを介して接続されたサーバから取得したプレフィクスに基づいて、匿名アドレスを生成し、
当該受信パケットの送信元アドレスを前記匿名アドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出し、
前記サーバは、
前記匿名化装置から送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第2のネットワークに転送する

ことを特徴とする通信方法。

[請求項20]

前記サーバが前記カプセル化パケットをデカプセル化して前記第2のネットワークに転送する際、

送信先アドレスが前記匿名アドレスであるパケットを受信した場合に、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記サーバのアドレスとし、かつ、送信先アドレスを前記匿名化装置のアドレスとして当該カプセル化パケットを前記第2のネットワークに転送し、

前記匿名装置は前記パケットを送出する際、

前記サーバから送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信先アドレスを前記通信ノードのアドレスとして前記第1のネットワークに送出する

ことを特徴とする請求項19に記載の通信方法。

[請求項21]

匿名化装置は、

第1のネットワークを介して接続された通信ノードから送信されたパケットを受信した場合に、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記匿名化装置とサーバとを接続する第2のネットワークに送出し、

前記匿名化装置と第2のネットワークを介して接続されたサーバは、

前記匿名化装置から送信されたカプセル化パケットを受信した場合に、

プレフィクスに基づいて、匿名アドレスを生成し、

当該カプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信元アドレスを前記匿名アドレスに書き換えた後に、当該デカプセル化パケットの送信元アドレスを前記匿名化装置のアドレスと

して前記第2のネットワークに送出する

ことを特徴とする通信方法。

[請求項22]

前記サーバが前記パケットを送出する際、

送信先アドレスが前記匿名アドレスであるパケットを受信した場合に、当該受信パケットの送信先アドレスを前記通信ノードのアドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記サーバのアドレスとし、かつ、送信先アドレスを前記匿名化装置のアドレスとして当該カプセル化パケットを前記第2のネットワークに送出し、

前記匿名装置が前記パケットを送出する際、

前記サーバから送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第1のネットワークに送出する

ことを特徴とする請求項21に記載の通信方法。

[請求項23]

第1のネットワークを介して接続される通信ノードから送信されたパケットを受信した場合に、第2のネットワークを介して接続されるサーバから取得したプレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、

前記通信ノードからの送信されたパケットの送信元アドレスを前記匿名アドレスに書き換え、当該パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを自身のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備える匿名化装置。

[請求項24]

匿名化装置と第1のネットワークを介して接続される通信ノードから送信されたパケットであって、かつ、前記匿名化装置によりカプセル化された後に第2のネットワークを介して送信されたパケットを受信した場合に、プレフィクスに基づいて、匿名アドレスを生成する匿名アドレス生成手段と、

前記匿名化装置から送信されたカプセル化パケットをデカプセル化し、当該デカプセル化パケットの送信元アドレスを前記匿名アドレスに書き換えた後に、当該デカプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとして前記第2のネットワークに送出するパケット処理手段と、を備えるサーバ。

[請求項25]

通信ノードと第1のネットワークを介して接続される匿名化装置と、当該匿名化装置と第2のネットワークを介して接続されるサーバと、を有し、

前記匿名化装置は、

前記通信ノードから送信されたパケットを受信した場合に、当該受信パケットの送信元アドレスを前記サーバから取得した匿名アドレスに書き換え、当該受信パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを前記匿名化装置のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段を備え、

前記サーバは、

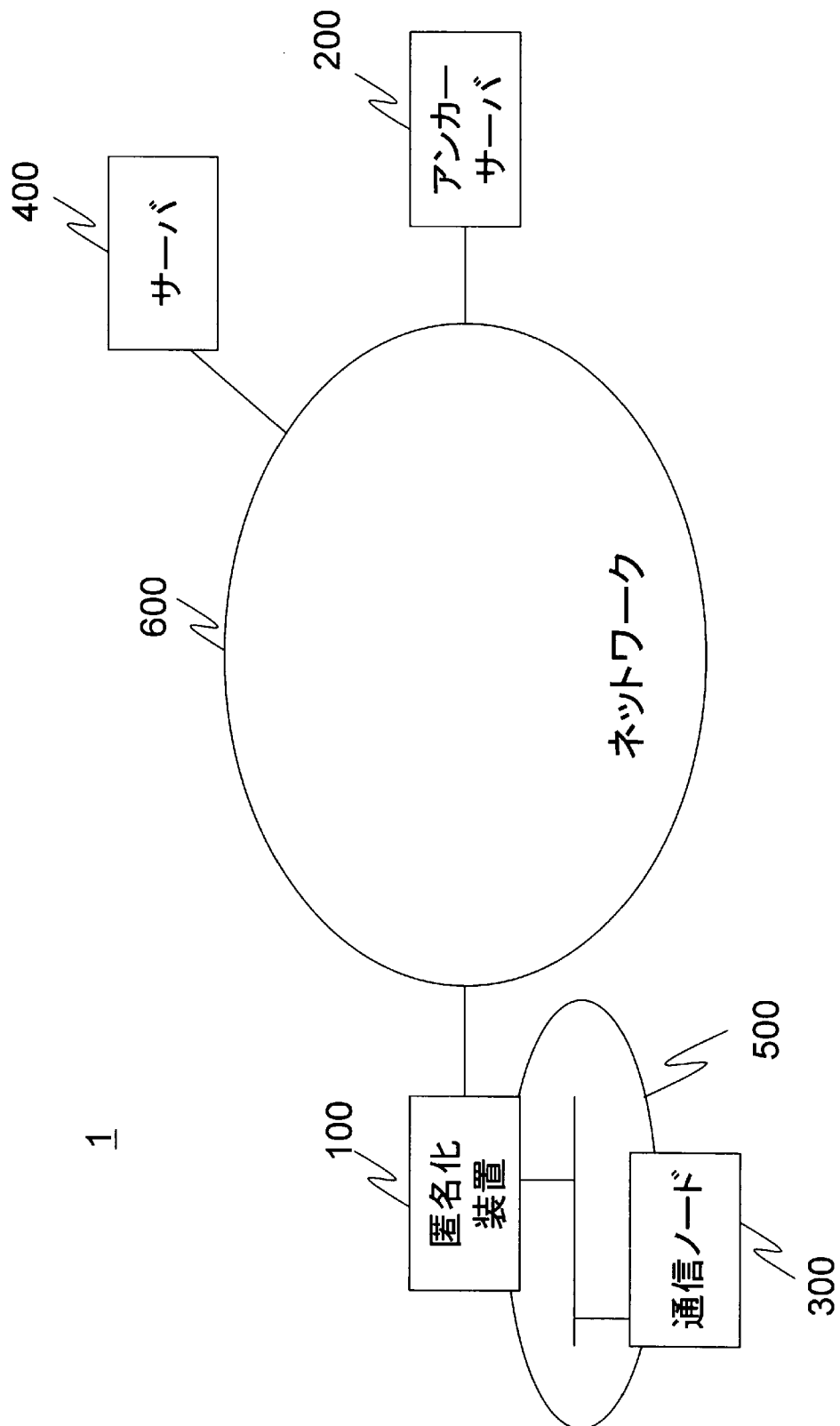
前記匿名化装置から送信された前記カプセル化パケットを受信した場合に、当該カプセル化パケットをデカプセル化して前記第2のネットワークに送出する転送手段を備える

ことを特徴とする通信システム。

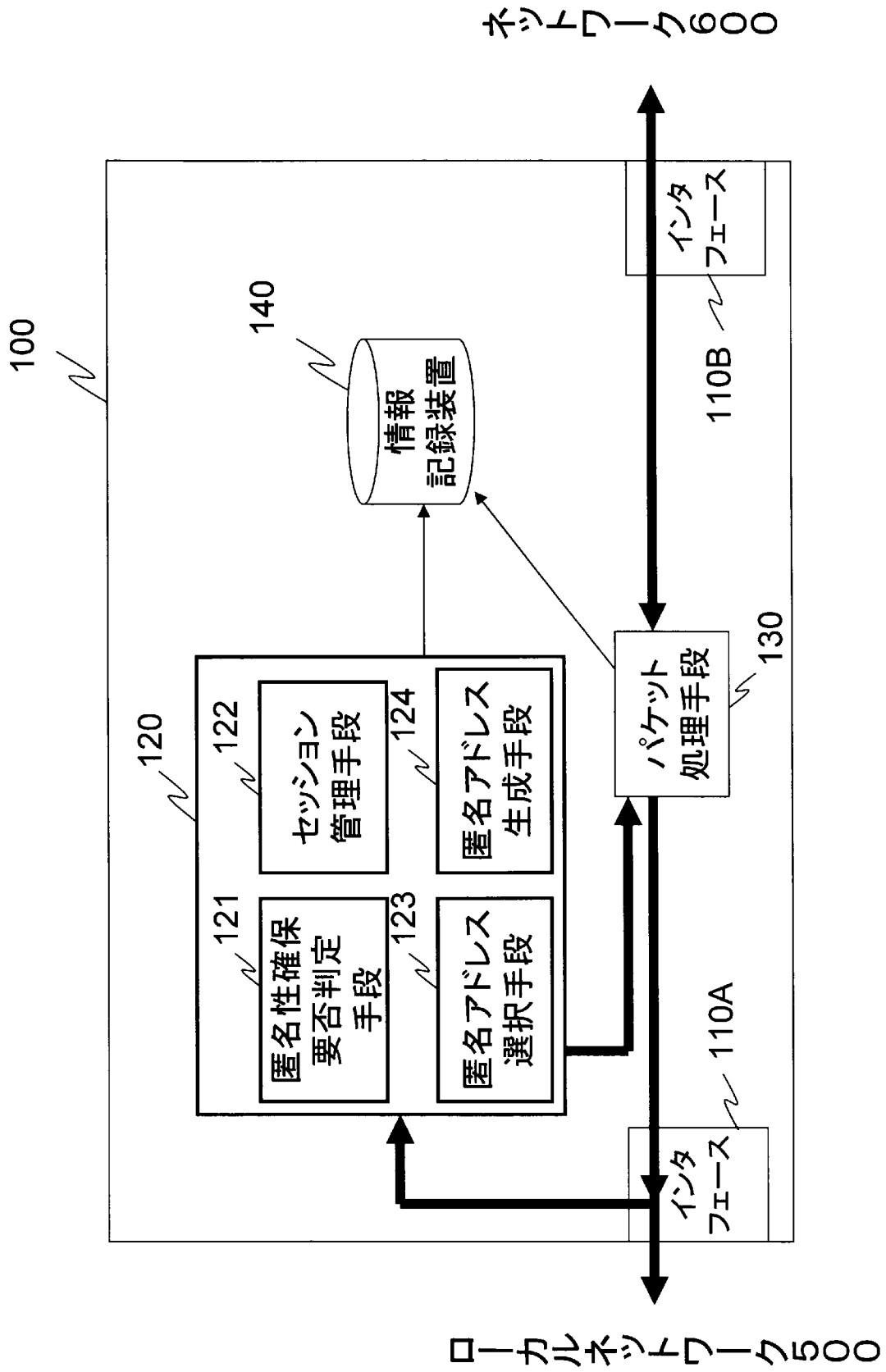
[請求項26]

第1のネットワークを介して接続される通信ノードから送信されたパケットを受信した場合に、第2のネットワークを介して接続されるサーバから匿名アドレスを取得し、前記通信ノードからの送信されたパケットの送信元アドレスを前記取得した匿名アドレスに書き換え、当該パケットをカプセル化した後に、当該カプセル化パケットの送信元アドレスを自身のアドレスとし、かつ、送信先アドレスを前記サーバのアドレスとして前記第2のネットワークに送出するパケット処理手段を備える匿名化装置。

[図1]



[図2]



[図3]

匿名化ポリシーテーブル

No	宛先アドレス	送信元アドレス	宛先 ポート	送信元 ポート	プロトコル	匿名化 要否
1	Sv_ADR1	any	80	any	TCP	Yes
2	Sv_ADR2	any	443	any	TCP	Yes
3	Sv_ADR3	any	80	any	TCP	Yes
4	any	any	any	any	TCP	No

[図4]

セッション管理テーブル

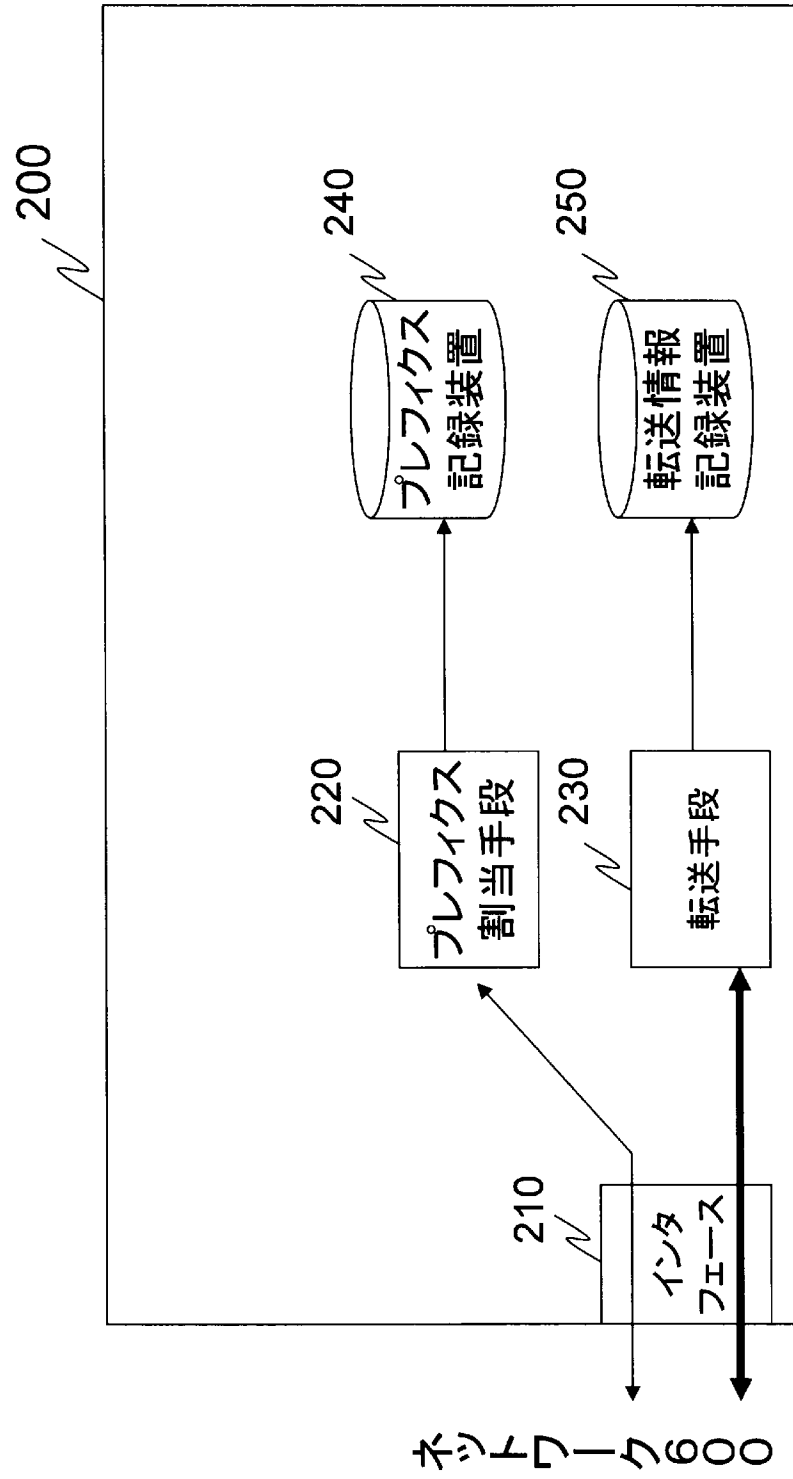
No	宛先 アドレス	送信元 アドレス	匿名 アドレス	宛先 ポート	送信元 ポート	プロトコ ル	アンカーサーバ アドレス	失効時刻
1	Sv_ADR1	Cl_ADR1	An_ADR1	80	10100	TCP	Anch_ADR1	expire_time1
2	Sv_ADR2	Cl_ADR1	An_ADR2	443	10105	TCP	Anch_ADR2	expire_time2
3	Sv_ADR2	Cl_ADR1	An_ADR3	80	10210	TCP	Anch_ADR1	expire_time3

[図5]

匿名化装置中のプレフィクス情報テーブル例

アンカー サーバ アドレス	プレフィクス セット番号	プレフィクス (プレフィクス長)	IID Key	割当 状態	割当終了 時刻	失効時刻
Anch_ADR1	1	Pref_A1 (64)	Key_A1	Y	-	expire_time_A1
		Pref_A2 (64)	Key_A2	Y	-	expire_time_A2
		Pref_A3 (64)	Key_A3	N	asgn_timeA3	expire_time_A3
Anch_ADR2	5	Pref_B9 (64)	Key_B9	N	asgn_timeB1	expire_time_B1
		Pref_B10 (64)	Key_B10	Y	-	expire_time_B2

[図6]



[図7]

貸出しプレフィクステーブル

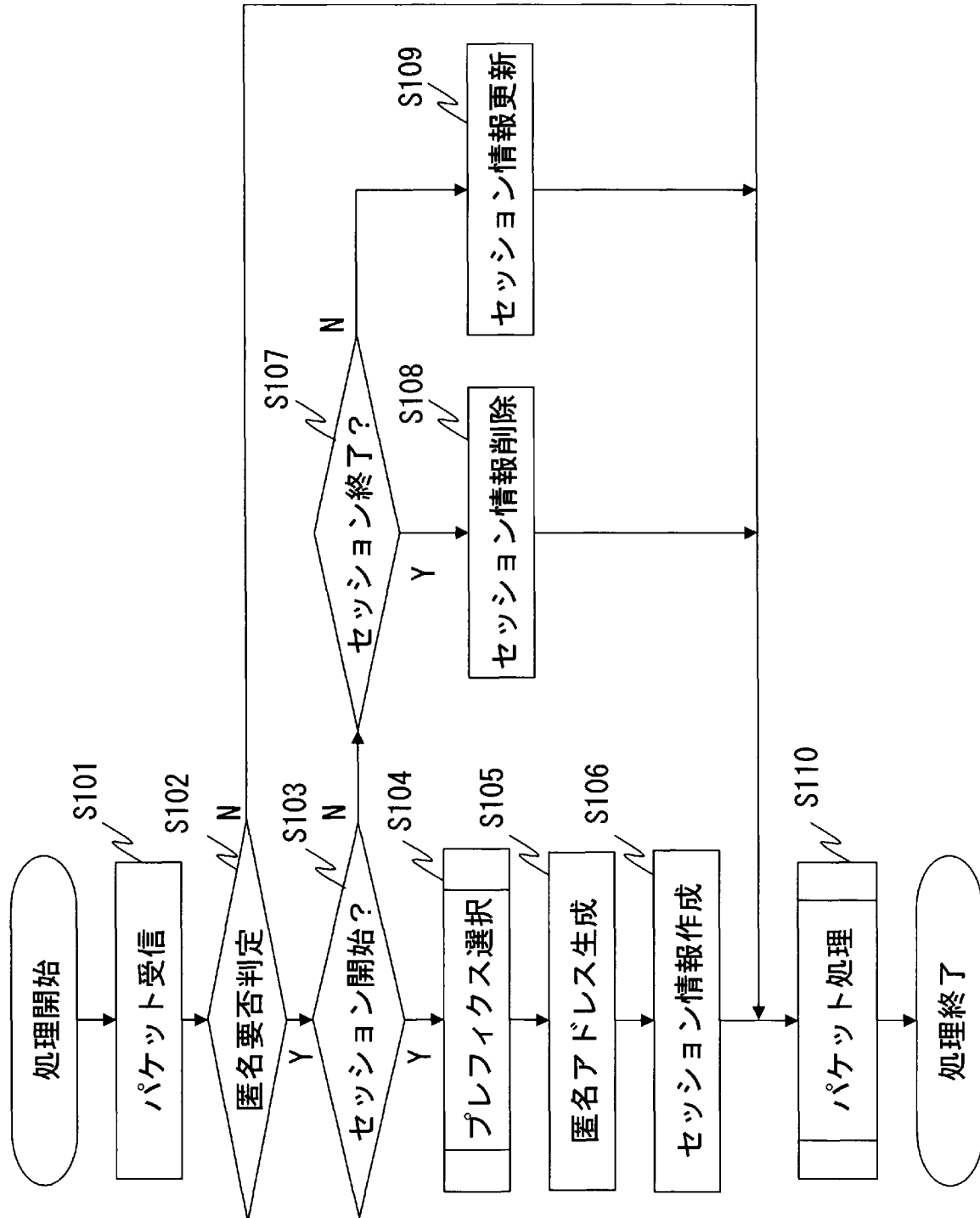
プレフィクスセット番号	プレフィクス	IID Key
1	Pref_A1 (64)	Key_A1
	Pref_A2 (64)	Key_A2
	Pref_A3 (64)	Key_A3
2	Pref_A4 (64)	Key_A4
	Pref_A5 (64)	Key_A5
	Pref_A6 (64)	Key_A6
3	Pref_A7 (64)	Key_A7
	Pref_A8 (64)	Key_A8
	Pref_A9 (64)	Key_A9

[図8]

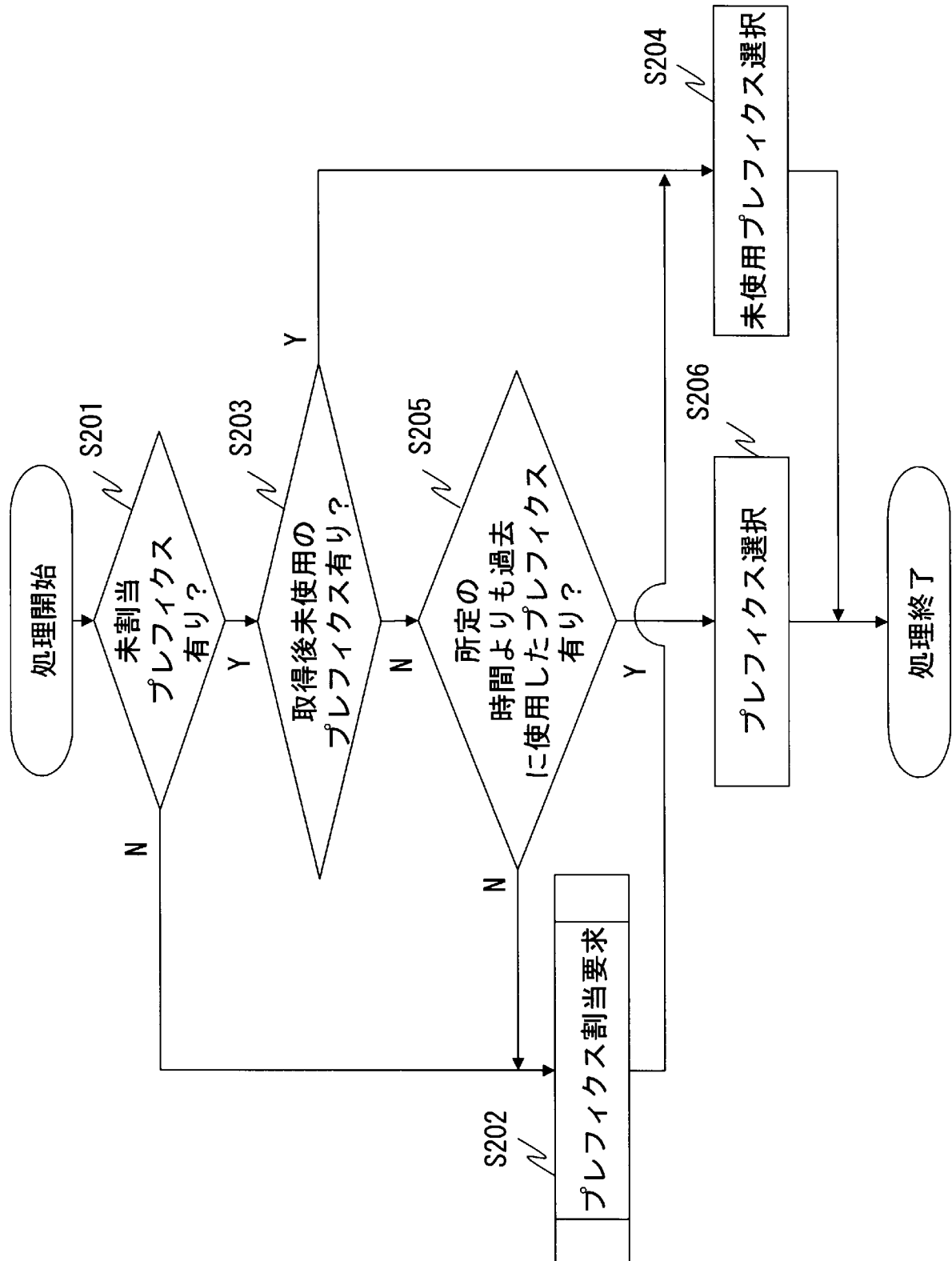
転送テーブル

No.	匿名アドレス	匿名化装置アドレス	失効時刻
1	An_ADR1	CPE_ADR1	expire_time1
2	An_ADR2	CPE_ADR1	expire_time2
3	An_ADR3	CPE_ADR1	expire_time3

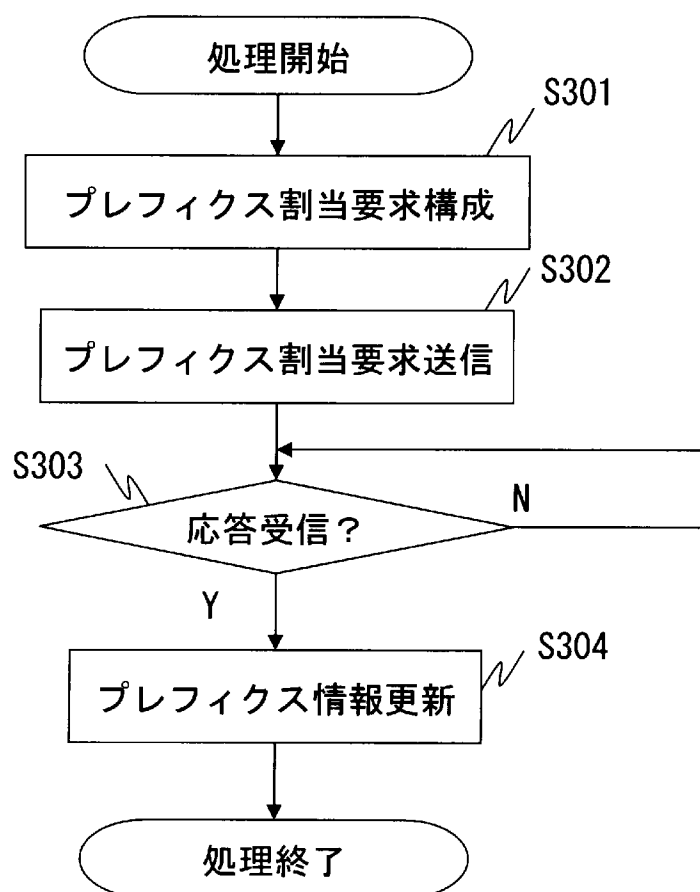
[図9]



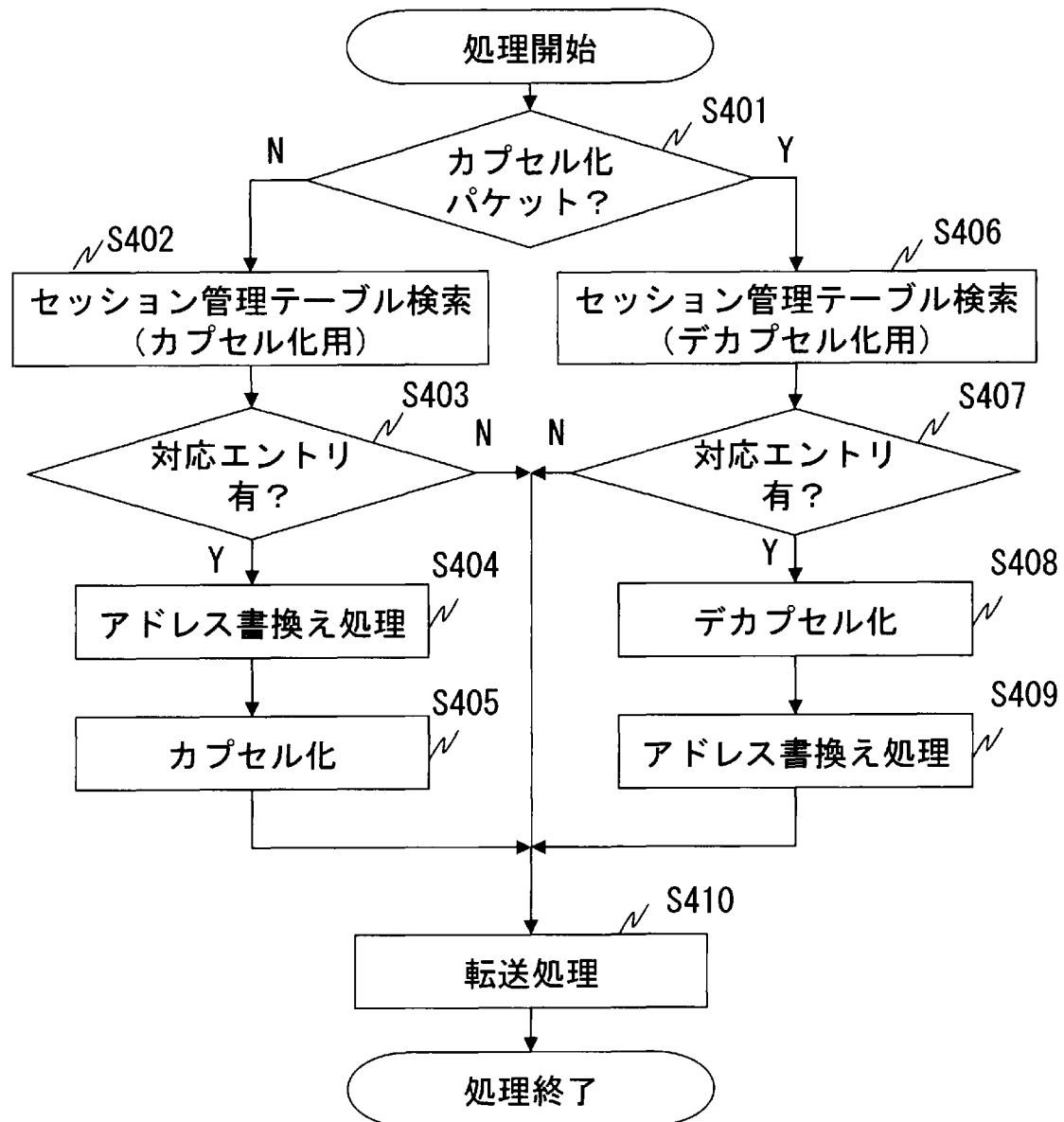
[図10]



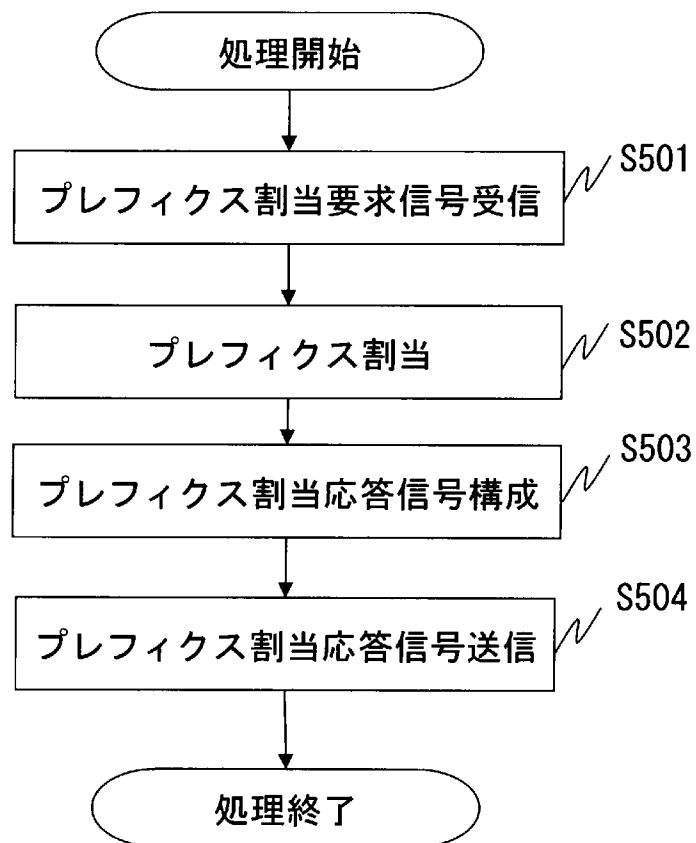
[図11]



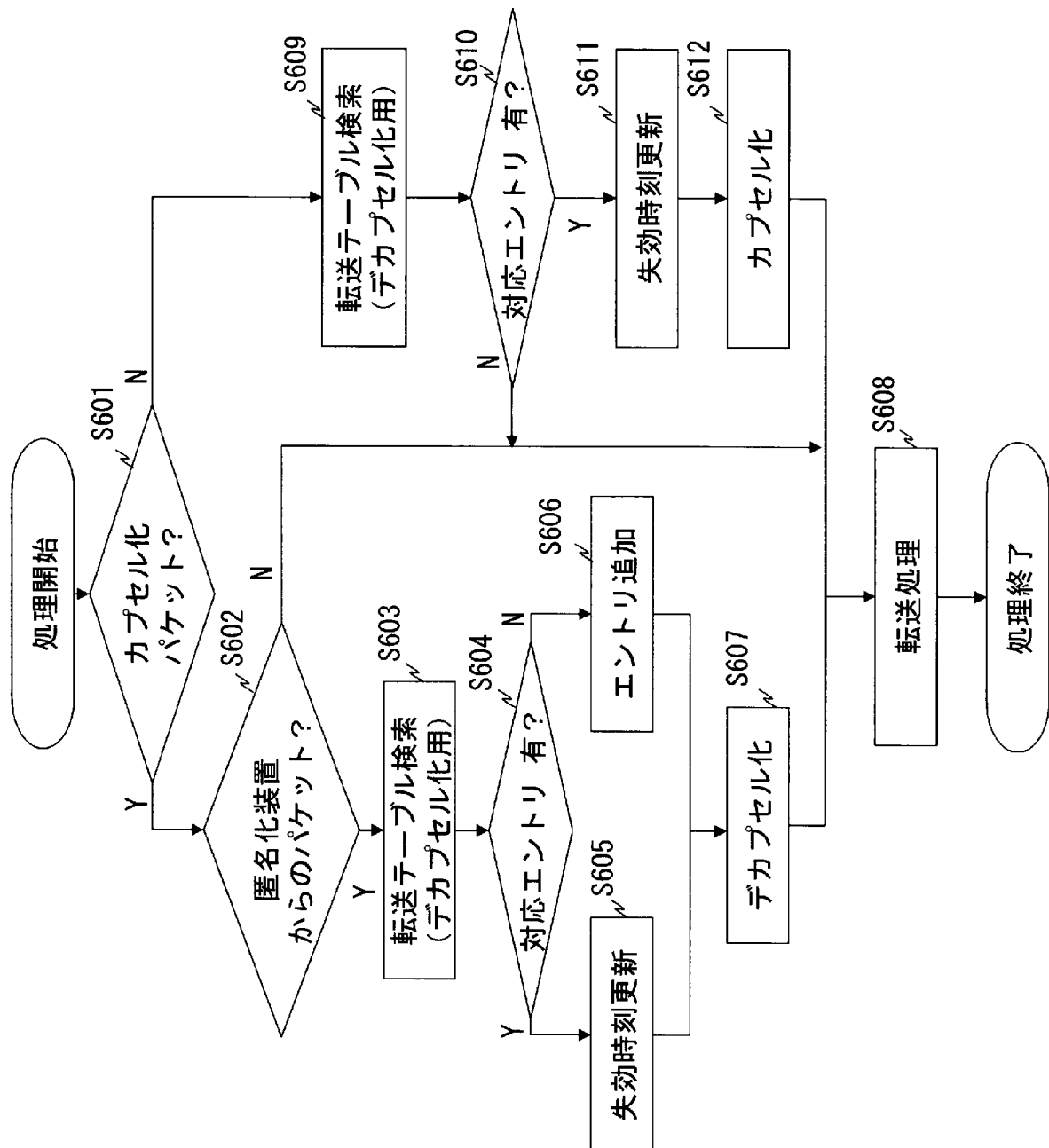
[図12]



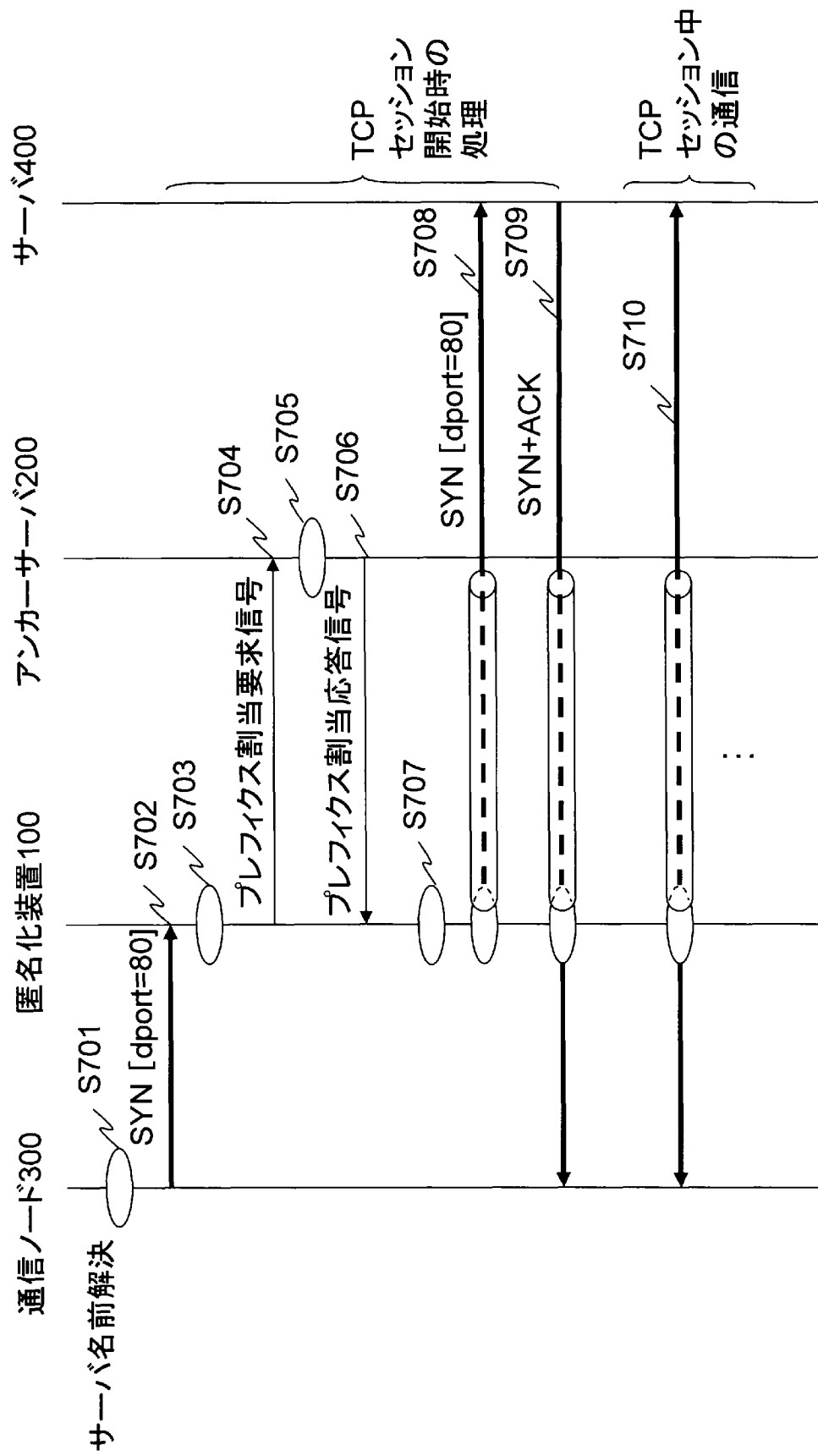
[図13]



[図14]



[図15]



[図16]

匿名化装置中のプレフィクス情報テーブル例

アンカーサーバー アドレス	プレフィク スセット 番号	プレフィクス (プレフィクス長)	IID Key	割当 状態	割当終了 時刻	失効時刻
Anch_ADR1	1	Pref_A1 (64)	Key_A1	Y	-	expire_time_A1
		Pref_A2 (64)	Key_A2	Y	-	expire_time_A2
		Pref_A3 (64)	Key_A3	N	asgn_timeA3	expire_time_A3
	2	Pref_A4 (64)	Key_A4	N	-	expire_time_A4
		Pref_A5 (64)	Key_A5	N	-	expire_time_A5
		Pref_A6 (64)	Key_A6	N	-	expire_time_A6
Anch_ADR2	5	Pref_B9 (64)	Key_B9	N	asgn_timeB1	expire_time_B1
		Pref_B10 (64)	Key_B10	Y	-	expire_time_B2

[図17]

セッション管理テーブル

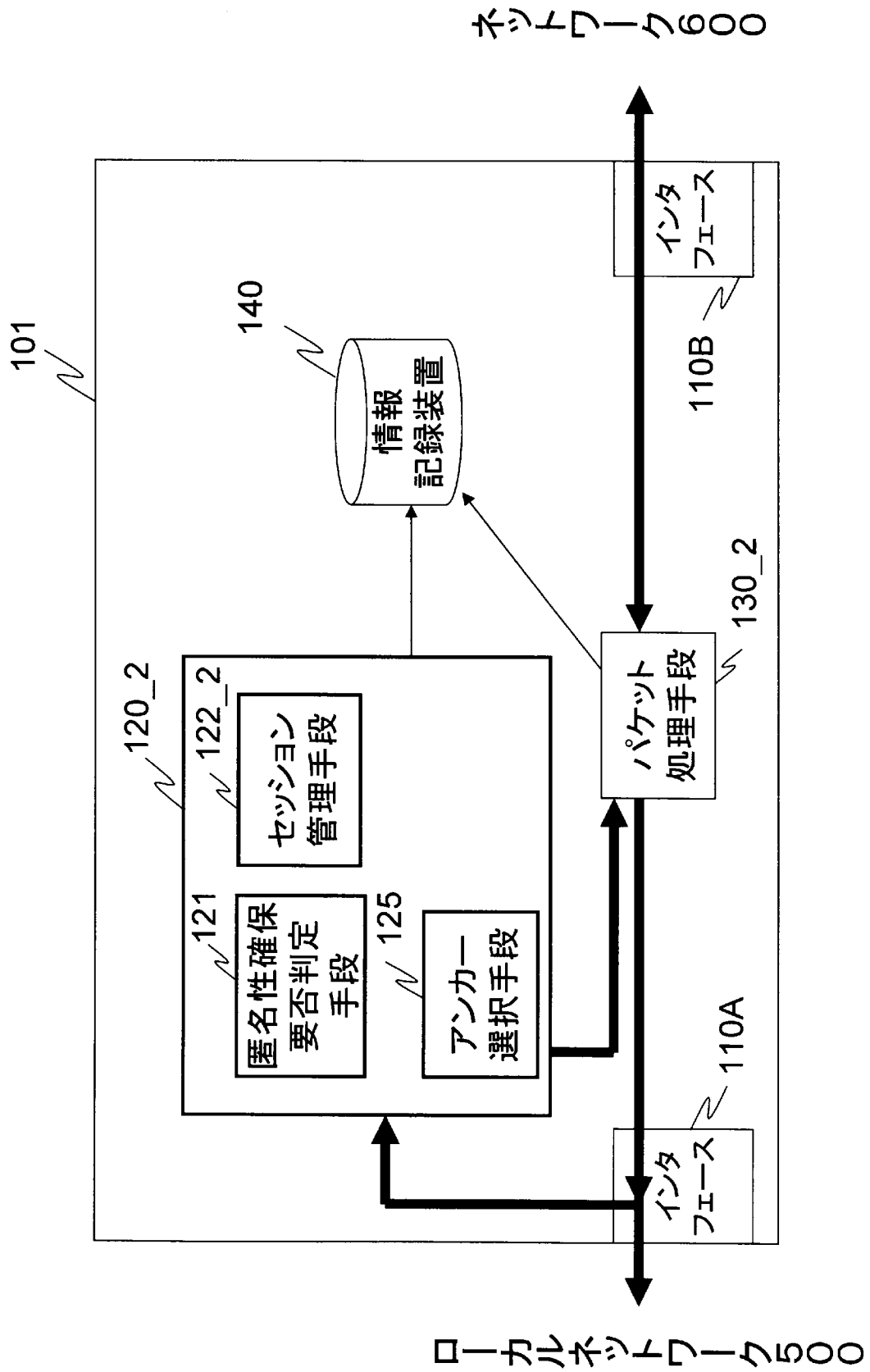
No	宛先 アドレス	送信元 アドレス	匿名 アドレス	宛先 ポート	送信元 ポート	プロトコル	アンカーサーバ アドレス	失効時刻
1	Sv_ADR1	Cl_ADR1	An_ADR1	80	10100	TCP	Anch_ADR1	expire_time1
2	Sv_ADR2	Cl_ADR1	An_ADR2	443	10105	TCP	Anch_ADR2	expire_time2
3	Sv_ADR2	Cl_ADR1	An_ADR3	80	10210	TCP	Anch_ADR1	expire_time3
4	Sv_ADR1	Cl_ADR1	An_ADR4	80	20000	TCP	Anch_ADR1	expire_time4

[図18]

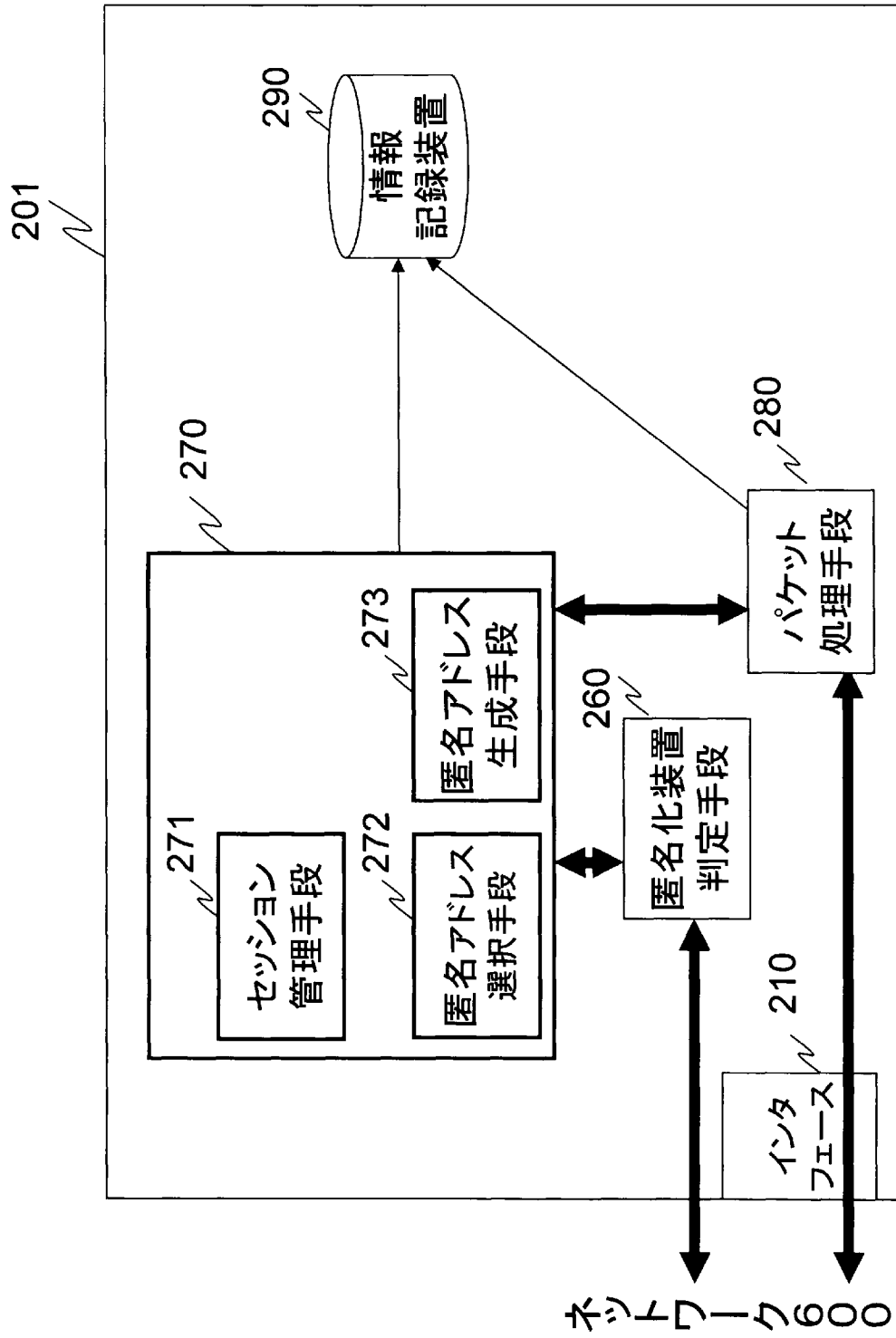
転送テーブル

No.	匿名アドレス	匿名化装置アドレス	失効時刻
1	An_ADR1	CPE_ADR1	expire_time1
2	An_ADR2	CPE_ADR1	expire_time2
3	An_ADR3	CPE_ADR1	expire_time3
4	An_ADR4	CPE_ADR1	expire_time4

[図19]



[図20]



[図21]

セッション管理テーブル

No	宛先 アドレス	送信元 アドレス	宛先 ポート	送信元 ポート	プロトコル	アンカーサーバーバ アドレス	失効時刻
1	Sv_ADR1	Cl_ADR1	80	10100	TCP	Anch_ADR1	expire_time1
2	Sv_ADR2	Cl_ADR1	443	10105	TCP	Anch_ADR2	expire_time2
3	Sv_ADR2	Cl_ADR1	80	10210	TCP	Anch_ADR1	expire_time3

[図22]

セッション管理テーブル

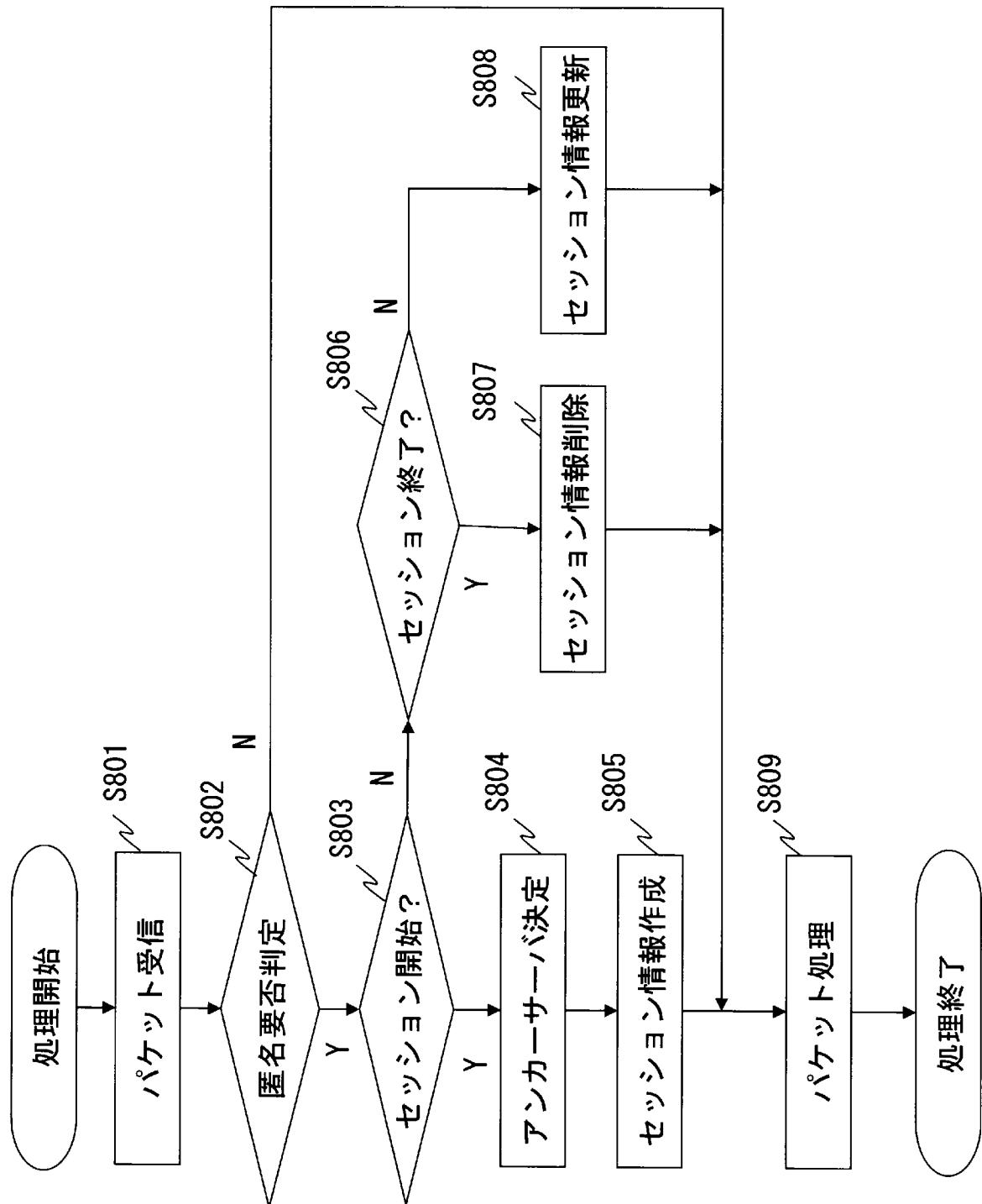
No	宛先 アドレス	送信元 アドレス	匿名 アドレス	宛先 ポート	送信元 ポート	プロトコル	匿名化装置 アドレス	失効時刻
1	Sv_ADR1	Cl_ADR1	An_ADR1	80	10100	TCP	CPE_ADR1	expire_time1
2	Sv_ADR2	Cl_ADR1	An_ADR2	443	10105	TCP	CPE_ADR2	expire_time2
3	Sv_ADR2	Cl_ADR1	An_ADR3	80	10210	TCP	CPE_ADR1	expire_time3

[図23]

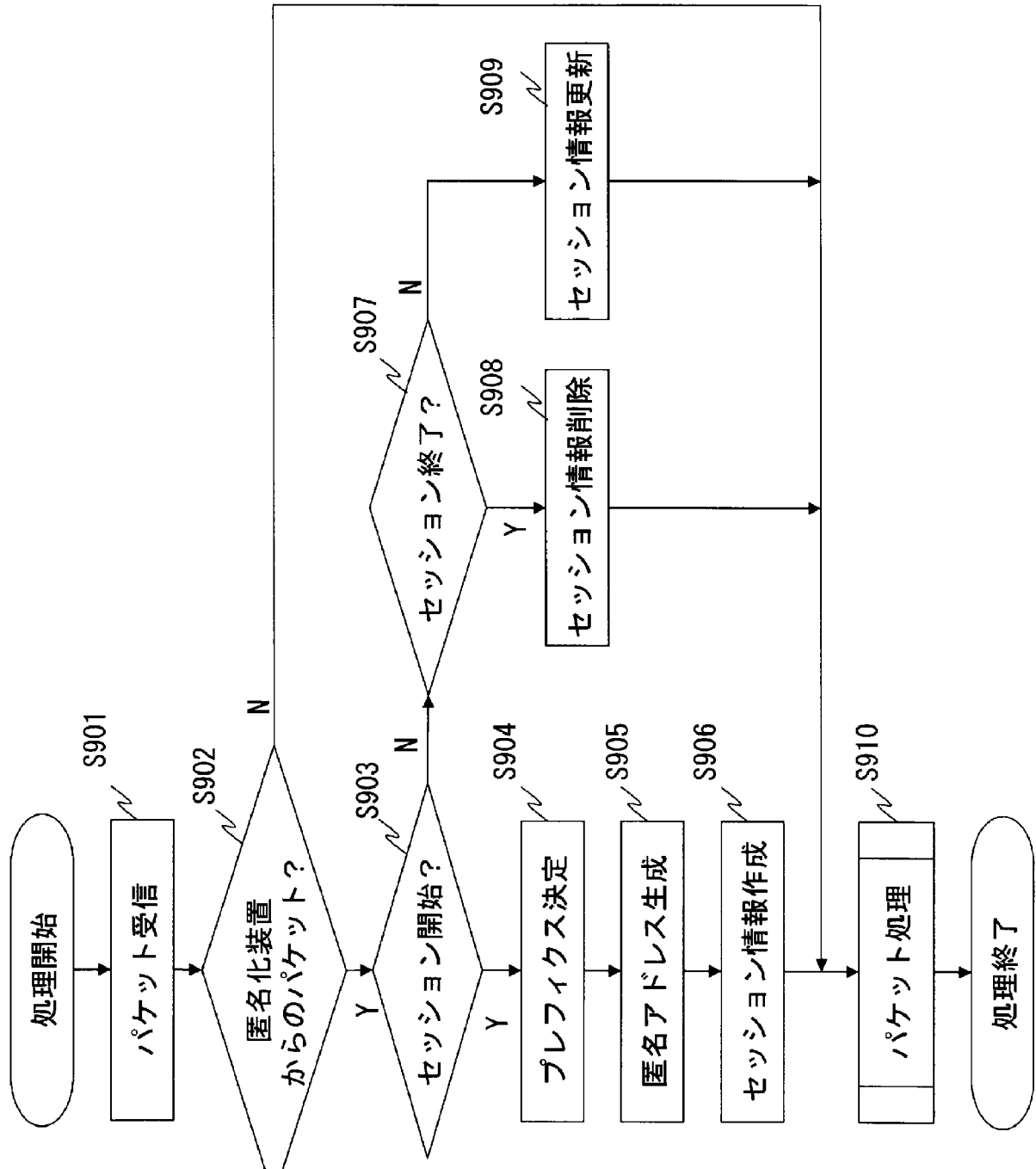
匿名化装置中のプレフィクス情報テーブル

プレフィクス	IID Key
Pref_A1	Key_A1
Pref_A2	Key_A2
Pref_A3	Key_A3
Pref_A4	Key_A4
Pref_A5	Key_A5

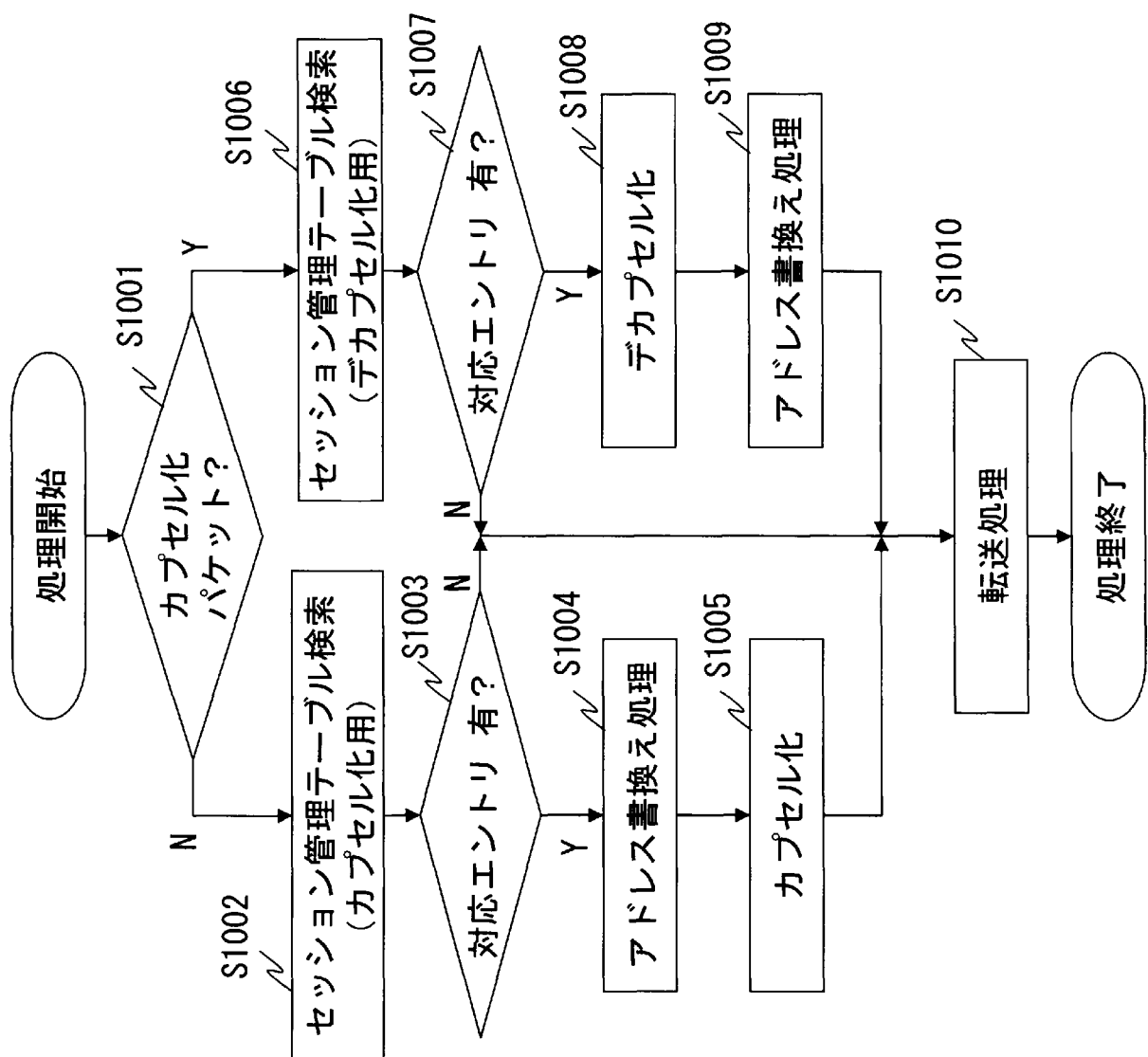
[図24]



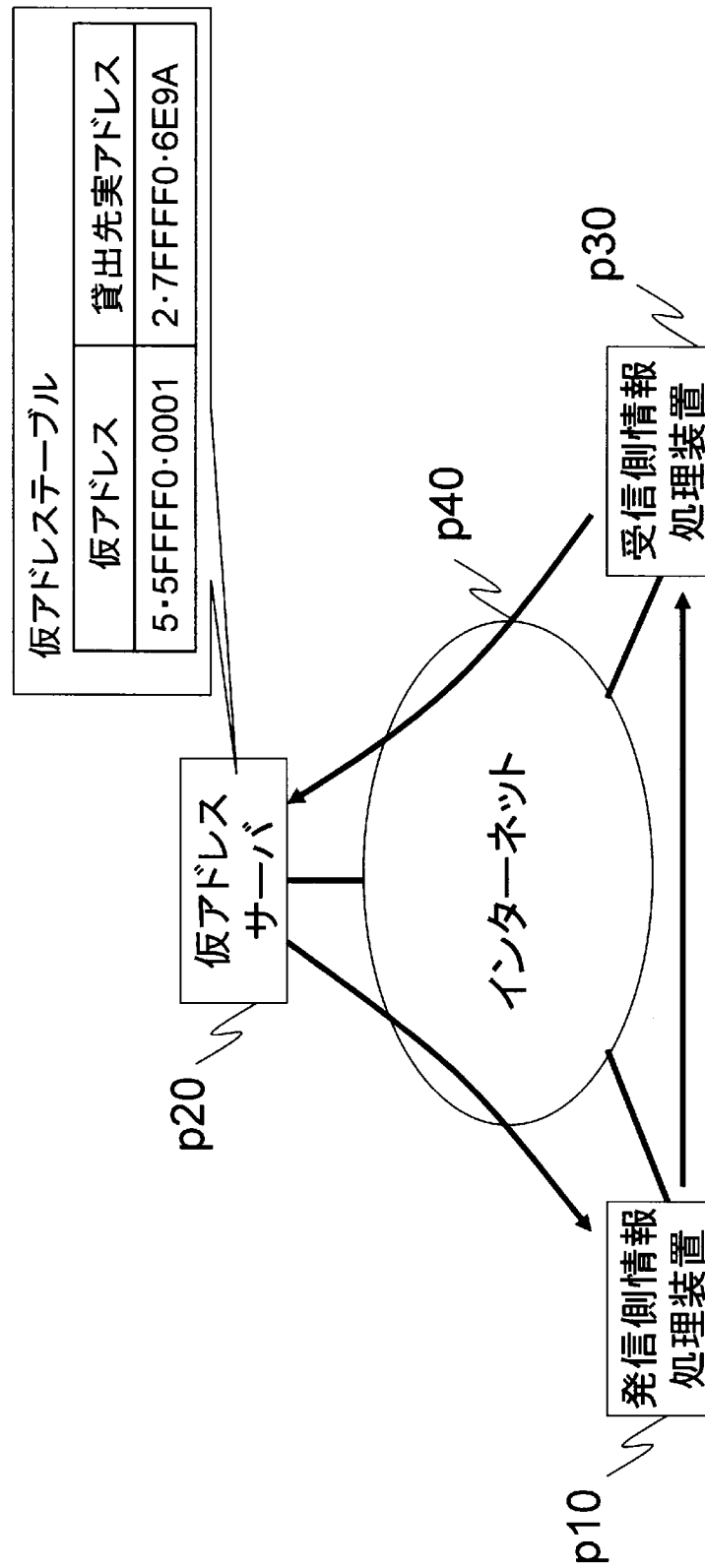
[図25]



[図26]



[図27]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/001110

A. CLASSIFICATION OF SUBJECT MATTER

H04L12/46(2006.01)i, H04L12/56(2006.01)i, H04L12/66(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L12/46, H04L12/56, H04L12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2003-298657 A (Toshiba Corp.), 17 October 2003 (17.10.2003), paragraphs [0017] to [0105] & US 2003/0185198 A1	1-26
Y	JP 2003-078551 A (Sharp Corp.), 14 March 2003 (14.03.2003), paragraphs [0057] to [0066] (Family: none)	1-26
Y	WO 2008/069100 A1 (NEC Corp.), 12 June 2008 (12.06.2008), paragraphs [0070] to [0076] (Family: none)	3, 13

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
27 April, 2010 (27.04.10)

Date of mailing of the international search report
11 May, 2010 (11.05.10)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2010/001110

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2008-098802 A (Seiko Epson Corp.), 24 April 2008 (24.04.2008), paragraph [0045] (Family: none)	4-7, 14, 15
A	JP 2006-005606 A (Hitachi, Ltd.), 05 January 2006 (05.01.2006), paragraphs [0014] to [0045] (Family: none)	1-26

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04L12/46(2006.01)i, H04L12/56(2006.01)i, H04L12/66(2006.01)i

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (I P C))

Int.Cl. H04L12/46, H04L12/56, H04L12/66

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 0 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 0 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 0 年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2003-298657 A (株式会社東芝) 2003. 10. 17, 段落【0017】-【0105】 & US 2003/0185198 A1	1-26
Y	JP 2003-078551 A (シャープ株式会社) 2003. 03. 14, 段落【0057】- 【0066】 (ファミリーなし)	1-26
Y	WO 2008/069100 A1 (日本電気株式会社) 2008. 06. 12, 段落 [0070]-[0076] (ファミリーなし)	3, 13

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

2 7 . 0 4 . 2 0 1 0

国際調査報告の発送日

1 1 . 0 5 . 2 0 1 0

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

脇水 佳弘

5 X

3 4 6 4

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 9 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y	JP 2008-098802 A (セイコーエプソン株式会社) 2008.04.24, 段落【0045】 (ファミリーなし)	4-7, 14, 15
A	JP 2006-005606 A (株式会社日立製作所) 2006.01.05, 段落【0014】 - 【0045】 (ファミリーなし)	1-26