(19)日本国特許庁(JP)　(12)特　許　公　報(B1)　(11)特許番号

特許第4843116号
(P4843116)

(45)発行日　平成23年12月21日(2011.12.21)　(24)登録日　平成23年10月14日(2011.10.14)

(51)Int.Cl.　　F I
H04L 12/46 (2006.01)　　H04L 12/46　A
H04L 9/14 (2006.01)　　H04L 9/00　641

請求項の数 12　(全 45 頁)

(21)出願番号　特願2011-180215 (P2011-180215)
(22)出願日　平成23年8月22日 (2011.8.22)
審査請求日　平成23年8月26日 (2011.8.26)

早期審査対象出願

(73)特許権者　510331951
株式会社ＩＮＴＯ
東京都新宿区新宿五丁目８番２０号
(74)代理人　110000925
特許業務法人信友国際特許事務所
(72)発明者　小川　恵子
東京都新宿区新宿五丁目８番２０号　株式会社ＩＮＴＯ内

審査官　中木　努

最終頁に続く

(54)【発明の名称】ネットワークゲートウェイ装置

(57)【特許請求の範囲】
【請求項１】
第一のＮＩＣと、
第二のＮＩＣと、
前記第一のＮＩＣ及び前記第二のＮＩＣにプロミスキャスモードを設定する初期設定部と、
前記第一のＮＩＣ及び前記第二のＮＩＣとの間でＴＣＰ／ＩＰ通信処理を行うＴＣＰ／ＩＰプロトコルスタックと、
前記第一のＮＩＣから受信した受信パケットに付されている送信元ＭＡＣアドレスを第一仮ＭＡＣアドレスに変換し、送信元ＩＰアドレスを第一仮ＩＰアドレスに変換し、宛先ＭＡＣアドレスを前記第一のＮＩＣに付されている第一のＮＩＣＭＡＣアドレスに変換し、宛先ＩＰアドレスを前記第一のＮＩＣに付されている第一のＮＩＣＩＰアドレスに変換して、前記ＴＣＰ／ＩＰプロトコルスタックに前記受信パケットを送信すると共に、前記ＴＣＰ／ＩＰプロトコルスタックから受信した送信パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを前記受信パケットに付されていた前記送信元ＭＡＣアドレス、前記送信元ＩＰアドレス、前記宛先ＭＡＣアドレス及び前記宛先ＩＰアドレスに書き戻して前記第二のＮＩＣに送信するアドレス変換処理部と
を具備するネットワークゲートウェイ装置。
【請求項２】

更に、
前記受信パケットに付されている前記送信元ＭＡＣアドレスを格納する送信元ＭＡＣアドレスフィールドと、前記受信パケットに付されている前記送信元ＩＰアドレスを格納する送信元ＩＰアドレスフィールドと、前記受信パケットに付されている前記宛先ＭＡＣアドレスを格納する宛先ＭＡＣアドレスフィールドと、前記受信パケットに付されている前記宛先ＩＰアドレスを記録する宛先ＩＰアドレスフィールドと、一意性を有する索引用の索引用ポート番号を記録する索引用ポート番号フィールドとを備えるアドレス変換テーブルと
を備え、
前記アドレス変換処理部は前記受信パケットに付されている送信元ポート番号を前記索引用ポート番号フィールドに記録した前記索引用ポート番号に変換すると共に、前記送信パケットに付されている宛先ポート番号で前記アドレス変換テーブルの前記索引用ポート番号フィールドを検索して、書き戻すべきレコードを特定する、
請求項１記載のネットワークゲートウェイ装置。
【請求項３】
更に、
前記ＴＣＰ／ＩＰプロトコルスタックから受信した受信パケットのペイロード部分に所定の暗号化処理を施して再度前記ＴＣＰ／ＩＰプロトコルスタックに返送する拡張ＴＣＰ処理部と
を備える、請求項２記載のネットワークゲートウェイ装置。
【請求項４】
更に、
前記第一のＮＩＣに対して第一のＴＣＰコネクションを形成するためのサーバ機能と、前記第二のＮＩＣに対して第二のＴＣＰコネクションを形成するためのクライアント機能とを備えると共に、前記第一のＮＩＣからＴＣＰ　ＦＩＮパケットが来たら、前記第二のＮＩＣからＴＣＰ　ＦＩＮパケットが来たことを検出して、前記第一のＴＣＰコネクションを切断する指示を前記ＴＣＰ／ＩＰプロトコルスタックに送るソケット処理部と
を備える、請求項３記載のネットワークゲートウェイ装置。
【請求項５】
前記アドレス変換処理部は、前記第一のＮＩＣからＴＣＰ　ＳＹＮパケットが来たら、前記アドレス変換テーブルにレコードを追加する、
請求項４記載のネットワークゲートウェイ装置。
【請求項６】
前記拡張ＴＣＰ処理部は、前記第一のＴＣＰコネクションから生じて前記ソケット処理部に到達しようとするストリームデータに前記暗号化処理を施した後、前記第二のＴＣＰコネクションに転送する、請求項５記載のネットワークゲートウェイ装置。
【請求項７】
前記アドレス変換処理部は、前記第一のＮＩＣからＴＣＰ　ＳＹＮパケットが来たことに呼応して前記第二のＴＣＰコネクションが形成される際、前記ＴＣＰ／ＩＰプロトコルスタックから発されるＡＲＰ要求パケットを受信すると、前記ＴＣＰ／ＩＰプロトコルスタックに対して偽のＭＡＣアドレスを含む擬似ＡＲＰ応答パケットを返信する、請求項４記載のネットワークゲートウェイ装置。
【請求項８】
前記アドレス変換処理部は、前記第一のＮＩＣからＴＣＰ　ＳＹＮパケットが来たら、前記アドレス変換テーブルにレコードを追加する、
請求項２記載のネットワークゲートウェイ装置。
【請求項９】
更に、
前記ＴＣＰ／ＩＰプロトコルスタックから受信した受信パケットのペイロード部分に所定の暗号化処理を施して再度前記ＴＣＰ／ＩＰプロトコルスタックに返送する拡張ＴＣＰ

処理部と
を備える、請求項８記載のネットワークゲートウェイ装置。
【請求項１０】
更に、
前記受信パケットに付されている前記送信元ＭＡＣアドレスを格納する第一の送信元ＭＡＣアドレスフィールドと、前記受信パケットに付されている前記送信元ＩＰアドレスを格納する第一の送信元ＩＰアドレスフィールドと、前記受信パケットに付されている前記宛先ＭＡＣアドレスを格納する第一の宛先ＭＡＣアドレスフィールドと、前記受信パケットに付されている前記宛先ＩＰアドレスを記録する第一の宛先ＩＰアドレスフィールドと、一意性を有する索引用の索引用ポート番号を記録する第一の索引用ポート番号フィールドとを備える第一のＮＩＣアドレス変換テーブルと、
第二の送信元ＭＡＣアドレスフィールドと、第二の送信元ＩＰアドレスフィールドと、第二の宛先ＭＡＣアドレスフィールドと、第二の宛先ＩＰアドレスフィールドと、前記索引用ポート番号を記録する第二の索引用ポート番号フィールドと、前記ＴＣＰ／ＩＰプロトコルスタックが生成する動的ポート番号を記録する動的ポート番号フィールドとを備える第二のＮＩＣアドレス変換テーブルと
を備え、
前記アドレス変換処理部は前記受信パケットに付されている送信元ポート番号を前記第一のＮＩＣアドレス変換テーブルの前記第一の索引用ポート番号フィールドに記録した前記索引用ポート番号に変換すると共に、前記送信パケットに付されている宛先ポート番号で前記第二のＮＩＣアドレス変換テーブルの前記第二の索引用ポート番号フィールドを検索して、書き戻すべきレコードを特定する、
請求項１記載のネットワークゲートウェイ装置。
【請求項１１】
更に、
送信元ＩＰアドレスフィールドと、送信元ポート番号フィールドと、宛先ＩＰアドレスフィールドと、宛先ポート番号フィールドとを有する拡張ＴＣＰ処理対象マスタと
を備え、
前記アドレス変換処理部は、前記第一のＮＩＣから受信したＴＣＰパケットの送信元及び宛先のＩＰアドレス及びポート番号の組み合わせが前記拡張ＴＣＰ処理対象マスタに登録されていれば、前記第一のＮＩＣから受信した受信パケットに付されている前記送信元ＭＡＣアドレス、前記送信元ＩＰアドレス、前記宛先ＭＡＣアドレス及び前記宛先ＩＰアドレスを変換し、前記第一のＮＩＣから受信したパケットが前記拡張ＴＣＰ処理対象マスタに登録されていなければ、前記第一のＮＩＣから受信した受信パケットを前記第一のＮＩＣから第二のＮＩＣに転送する、
請求項１記載のネットワークゲートウェイ装置。
【請求項１２】
前記アドレス変換処理部は、
前記第一のＮＩＣから受信したＴＣＰパケットの送信元及び宛先のＩＰアドレス及びポート番号の組み合わせが前記拡張ＴＣＰ処理対象マスタに登録されていれば、前記第一のＮＩＣから受信した受信パケットに付されている前記送信元ＭＡＣアドレス、前記送信元ＩＰアドレス、前記宛先ＭＡＣアドレス及び前記宛先ＩＰアドレスを変換し、
前記第一のＮＩＣから受信したＴＣＰパケットが前記拡張ＴＣＰ処理対象マスタに登録されておらず、且つ前記ＴＣＰパケットの宛先ＩＰアドレスが前記第一のＮＩＣに本来付されているＩＰアドレスである場合は、前記ＴＣＰパケットをそのまま前記ＴＣＰ／ＩＰプロトコルスタックに転送する、
請求項１１記載のネットワークゲートウェイ装置。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、ネットワークゲートウェイ装置に関する。
より詳細には、既存のネットワーク環境に対して何ら設定変更を強いることなく、容易にセキュリティを高めた暗号化通信機能を追加できるネットワークゲートウェイ装置に関する。
【背景技術】
【０００２】
発明者は、インターネットが爆発的に一般層に普及する早期の段階から、ＴＣＰ／ＩＰネットワークの可能性と技術的限界、そして問題点を認識していた。例えば、インターネットメールは基本的に葉書と同等であり、通信経路上でタッピング（tapping：盗聴）を行えば容易にメールヘッダ及び本文を取得できる。そして、インターネットメールやｗｅｂ等の通信アプリケーションに、セキュリティを向上させるための暗号化を行うに際しては、全てアプリケーションプログラムが対応していた。このため、暗号化通信に対応しているアプリケーションは暗号化通信に対応していないアプリケーションと暗号化通信を行うことはできず、いつまで経っても暗号化通信対応アプリケーションが普及しない、というジレンマに陥っていた。
【０００３】
また、暗号化通信環境がなかなか普及しない、という同様の問題点は、ネットワーク層で暗号化通信を実現するＩＰＳｅｃにも言える。アプリケーション層のアプローチではなく、ネットワーク層であらゆる通信を丸ごと暗号化する、というＩＰＳｅｃの基本的技術思想は良い着眼点であろう。しかし、現実には繋がり難い、繋がるまでの設定が大変である、通信が切れ易い、或はユーザ認証を別途考慮しなければならない等の問題点が指摘され、根本的な解決がなされず普及の目処も立たないまま現在に至っている。
【０００４】
このようなＴＣＰ／ＩＰネットワークの可能性と技術的限界、そして問題点に鑑み、発明者はトランスポート層で認証及び暗号化通信を実現する技術を発明し、今日に至るまでその技術の実装と改良に努めている。なお、本明細書ではこれ以降、特許文献１に開示した技術に基づく、トランスポート層における認証及び暗号化の技術を、ＴＣＰの拡張（ｅＸＰａｎｄ）という意味を込めて「ＸＰＴＣＰ」と称する。
特許文献１は、発明者によるトランスポート層の暗号化プロトコルに関する先行技術文献である。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特許３７８３１４２号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
特許文献１に開示したＸＰＴＣＰを既存のネットワーク環境に導入する際、その導入障壁はできるだけ低いことが好ましい。理想的には、ネットワーク上の全ての端末が「ゼロコンフィギュレーション(Zero Configuration）」、つまり全く設定等を変更したり新規のソフトウェアを導入することなく、ＸＰＴＣＰが提供する新たな機能を利用できるようになることが望ましい。
【０００７】
端末にソフトウェアを導入せずに新機能を実現する方法として、ネットワークの経路上にゲートウェイ装置を介入させる方法が考えられる。しかし、このゲートウェイ装置は、これまで知られている装置やアプリケーションの態様では、どうしても端末の設定変更が必要になる。
例えば、ゲートウェイ装置がプロキシサーバである場合、端末はプロキシサーバ対応アプリケーションプログラムを用いて、アプリケーションプログラムにはプロキシサーバのＩＰアドレスとポート番号を設定しなければならない。つまり、アプリケーションプログ

ラムがプロキシサーバに対応していないと、プロキシサーバを介した通信そのものが実現できない。

また例えば、ゲートウェイ装置がルータである場合、端末はデフォルトゲートウェイのＩＰアドレスを設定し直さなければならない。

更に、ゲートウェイ装置が既存のネットワーク環境に導入されることを考えると、ゲートウェイ装置のための空いているＩＰアドレスを確保しなければならない他、既にあるデフォルトゲートウェイとなっているルータ等、他のネットワーク装置にも設定変更が必要になることもある。

【０００８】

本発明はかかる課題を解決し、既存のネットワーク環境に対して設定変更を何ら強いることなく、容易にセキュリティを高めた暗号化通信機能を追加できるネットワークゲートウェイ装置を提供することを目的とする。

【課題を解決するための手段】

【０００９】

上記課題を解決するために、本発明のネットワークゲートウェイ装置は、内側ＮＩＣと、外側ＮＩＣと、内側ＮＩＣ及び外側ＮＩＣにプロミスキャスモードを設定する初期設定部と、内側ＮＩＣ及び外側ＮＩＣとの間でＴＣＰ／ＩＰ通信処理を行うＴＣＰ／ＩＰプロトコルスタックと、内側ＮＩＣから受信した受信パケットに付されている送信元ＭＡＣアドレスを第一偽装ＭＡＣアドレスに変換し、送信元ＩＰアドレスを第一偽装ＩＰアドレスに変換し、宛先ＭＡＣアドレスを内側ＮＩＣに付されている内側ＮＩＣＭＡＣアドレスに変換し、宛先ＩＰアドレスを内側ＮＩＣに付されている内側ＮＩＣＩＰアドレスに変換して、ＴＣＰ／ＩＰプロトコルスタックに受信パケットを送信すると共に、ＴＣＰ／ＩＰプロトコルスタックから受信した送信パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを受信パケットに付されていた送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスに書き戻して外側ＮＩＣに送信するアドレス変換処理部とを具備する。

【００１０】

内側ＮＩＣ及び外側ＮＩＣに割り当てられているＩＰアドレスとは無関係である筈のパケットをＴＣＰ／ＩＰプロトコルスタックが処理できるようにするために、受信パケットに付されている送信元ＭＡＣアドレス及び送信元ＩＰアドレスは偽のＭＡＣアドレス及び偽のＩＰアドレスに、宛先ＭＡＣアドレス及び宛先ＩＰアドレスは内側ＮＩＣに割り当てられているＩＰアドレス及びＭＡＣアドレスに書き換えてから、ＴＣＰ／ＩＰプロトコルスタックに与える。

【発明の効果】

【００１１】

本発明により、既存のネットワーク環境に対して設定変更を何ら強いることなく、容易にセキュリティを高めた暗号化通信機能を追加できるネットワークゲートウェイ装置を提供できる。

【図面の簡単な説明】

【００１２】

【図１】本発明の実施形態に係るネットワークゲートウェイ装置を含むネットワークの概略図である。

【図２】ＸＰＴＣＰゲートウェイ装置の機能ブロック図である。

【図３】ＸＰＴＣＰゲートウェイ装置に備わっている各種テーブル及びリストのフィールド構成を示す図である。

【図４】パケットの構造を示す概略図である。

【図５】アドレス変換処理部の機能ブロック図である。

【図６】内側ＮＩＣ受信処理部の機能ブロック図である。

【図７】外側ＮＩＣ受信処理部の機能ブロック図である。

【図８】外側ＮＩＣ送信処理部の機能ブロック図である。

【図９】内側ＮＩＣ送信処理部の機能ブロック図である。
【図１０】ＸＰＴＣＰ処理部の機能ブロック図である。
【図１１】アドレス変換処理部の、内側ＮＩＣにおけるパケット受信処理の動作の流れを示すフローチャートである。
【図１２】アドレス変換処理部の、外側ＮＩＣにおけるパケット受信処理の動作の流れを示すフローチャートである。
【図１３】アドレス変換処理部の、外側ＮＩＣにおけるパケット送信処理の動作の流れを示すフローチャートである。
【図１４】アドレス変換処理部の、内側ＮＩＣにおけるパケット送信処理の動作の流れを示すフローチャートである。
【図１５】ＸＰＴＣＰ処理部のＸＰＴＣＰ処理の流れを示すフローチャートである。
【図１６】ソケット処理部の初期動作の流れを示すフローチャートである。
【図１７】ソケット処理部の接続要求転送処理の流れを示すフローチャートである。
【図１８】ＸＰＴＣＰゲートウェイ装置を通過するパケットの変化を示す概略図である。
【図１９】ＸＰＴＣＰゲートウェイ装置を通過するパケットの変化を示す概略図である。
【図２０】ＸＰＴＣＰゲートウェイ装置を通過するパケットの変化を示す概略図である。
【図２１】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰ接続確立シーケンスを示すタイムチャートの、全体を示す俯瞰図である。
【図２２】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰ接続確立シーケンスを示すタイムチャートのうち、前半の処理内容を示す詳細図である。
【図２３】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰ接続確立シーケンスを示すタイムチャートのうち、後半の処理内容を示す詳細図である。
【図２４】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰデータ転送シーケンスのタイムチャートである。
【図２５】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰ切断シーケンスを示すタイムチャートの、全体を示す俯瞰図である。
【図２６】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰ切断シーケンスを示すタイムチャートのうち、前半の処理内容を示す詳細図である。
【図２７】ＸＰＴＣＰゲートウェイ装置における、ＴＣＰ切断シーケンスを示すタイムチャートのうち、後半の処理内容を示す詳細図である。
【図２８】ＸＰＴＣＰゲートウェイ装置において、送信するパケットの宛先ＩＰアドレスを書き換える応用形態を説明する概略図である。
【図２９】ＸＰＴＣＰゲートウェイ装置において、送信するパケットの送信元ＩＰアドレスを書き換える応用形態を説明する概略図である。
【発明を実施するための形態】
【００１３】
［ネットワークの概略］
図１は、本発明の実施形態に係るネットワークゲートウェイ装置を含むネットワークの概略図である。
本実施形態のネットワークゲートウェイ装置はＸＰＴＣＰ機能を提供するので、これ以降、ネットワークゲートウェイ装置をＸＰＴＣＰゲートウェイ装置１０１と称する。
図１には、ＸＰＴＣＰゲートウェイ装置１０１を含むネットワークが示されている。
ＸＰＴＣＰゲートウェイ装置１０１を介して左側には、ＸＰＴＣＰに非対応である二台の端末、ＸＰＴＣＰ非対応ＰＣ１０２及びＸＰＴＣＰ非対応ＰＣ１０３が、ＸＰＴＣＰゲートウェイ装置１０１の内側ＮＩＣ１０４に接続されている。
【００１４】
ＸＰＴＣＰゲートウェイ装置１０１を介して右側には、ＸＰＴＣＰに非対応の端末であるＸＰＴＣＰ非対応ＰＣ１０５と、ＸＰＴＣＰに対応している端末であるＸＰＴＣＰ対応ＰＣ１０６、及びＸＰＴＣＰに対応しているサーバであるＸＰＴＣＰ対応サーバ１０７が、ＸＰＴＣＰゲートウェイ装置１０１の外側ＮＩＣ１０８に接続されている。

これ以降、ＸＰＴＣＰゲートウェイ装置１０１を介して左側のネットワークをＸＰＴＣＰ非対応ネットワーク１０９と、ＸＰＴＣＰゲートウェイ装置１０１を介して右側のネットワークをＸＰＴＣＰ対応ネットワーク１１０と、それぞれ称する。

つまり、ＸＰＴＣＰゲートウェイ装置１０１は、第一のＮＩＣともいえる内側ＮＩＣ１０４がＸＰＴＣＰ非対応ネットワーク１０９に接続され、第二のＮＩＣともいえる外側ＮＩＣ１０８がＸＰＴＣＰ対応ネットワーク１１０に接続されている。

【００１５】

ＸＰＴＣＰゲートウェイ装置１０１は、ＸＰＴＣＰ非対応ネットワーク１０９に存在するＸＰＴＣＰ非対応ＰＣ１０２及びＸＰＴＣＰ非対応ＰＣ１０３のような、ＸＰＴＣＰ非対応のネットワーク機器を、ＸＰＴＣＰ対応ネットワーク１１０に存在するＸＰＴＣＰ対応ＰＣ１０６及びＸＰＴＣＰ対応サーバ１０７のような、ＸＰＴＣＰ対応のネットワーク機器に、ＸＰＴＣＰの機能を以て接続できるように、パケットを加工する。

【００１６】

ＸＰＴＣＰゲートウェイ装置１０１は、内側ＮＩＣ１０４に接続されているＸＰＴＣＰ非対応ＰＣ１０２に対し、ＸＰＴＣＰの機能を提供する。具体的には、ＸＰＴＣＰ非対応ネットワーク１０９上のＸＰＴＣＰ非対応ＰＣ１０２がＸＰＴＣＰ対応ネットワーク１１０上のＸＰＴＣＰ非対応ＰＣ１０５に接続しようとする場合には、ＸＰＴＣＰゲートウェイ装置１０１はパケットをそのまま流して、従来と同様の一般的なＴＣＰ／ＩＰネットワークにおける通信を行う。しかし、ＸＰＴＣＰ非対応ネットワーク１０９上のＸＰＴＣＰ非対応ＰＣ１０２がＸＰＴＣＰ対応ネットワーク１１０上のＸＰＴＣＰ対応ＰＣ１０６或はＸＰＴＣＰ対応サーバ１０７に接続しようとする場合には、ＸＰＴＣＰゲートウェイ装置１０１はＸＰＴＣＰ非対応ＰＣ１０２から送信されるパケットをＸＰＴＣＰに対応したパケットに書き換えて、ＸＰＴＣＰ対応ＰＣ１０６或はＸＰＴＣＰ対応サーバ１０７に送信する。

【００１７】

［ＸＰＴＣＰゲートウェイ装置１０１の内部構成］

図２はＸＰＴＣＰゲートウェイ装置１０１の機能ブロック図である。

ＸＰＴＣＰゲートウェイ装置１０１は、ネットワークＯＳが稼働するコンピュータにＸＰＴＣＰゲートウェイ装置１０１として稼働する為のプログラムを導入することで実現できる。ネットワークＯＳは、例えば周知のＷｉｎｄｏｗｓ（登録商標）或はＬｉｎｕｘ（登録商標）等のＯＳが利用可能である。但し、ＸＰＴＣＰゲートウェイ装置１０１はネットワークの経路上に設置される必要があるので、コンピュータには二つのＮＩＣ（Network Interface Card）が備わっている必要がある。これが内側ＮＩＣ１０４と外側ＮＩＣ１０８である。

【００１８】

内側ＮＩＣ１０４と外側ＮＩＣ１０８は、それぞれ周知のＴＣＰ／ＩＰネットワークに接続するための、一般的なインターフェースカードである。したがって、内側ＮＩＣ１０４と外側ＮＩＣ１０８にはそれぞれ周知且つ固有の、４８ビットのＭＡＣアドレス(Media Access Control address)を有する。なお、図２に機能ブロックとして示す内側ＮＩＣ１０４と外側ＮＩＣ１０８は、ハードウェアとしてのＮＩＣそのものに加え、デバイスドライバの機能も含んでいる。

初期設定部２０１は、ネットワークＯＳが起動した際に設定されるネットワークの基本設定作業に加えて、内側ＮＩＣ１０４と外側ＮＩＣ１０８に「プロミスキャスモード（promiscuous mode）」を設定する。「無差別モード」とも言われるこのモードは、ネットワーク上を流れる全てのパケットを受信して読み込むことができる。本実施形態のＸＰＴＣＰゲートウェイ装置１０１には必要な設定である。

【００１９】

図示しないネットワークＯＳは、起動の際にネットワークの基本設定を行う。その際の、内側ＮＩＣ１０４及び外側ＮＩＣ１０８のＭＡＣアドレス及びＩＰアドレスは、ネットワーク設定情報メモリ２０２に記憶される。

【００２０】
アドレス変換処理部２０３は、内側ＮＩＣ１０４から受信したパケットに対し、ネットワーク設定情報メモリ２０２、仮ＩＰＭＡＣリスト２０４及び内側ＮＩＣアドレステーブル２０９からそれぞれ情報を読み込み、パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを、第一仮ＮＩＣＭＡＣアドレス、第一仮ＮＩＣＩＰアドレス、索引用ポート番号、内側ＮＩＣＭＡＣアドレス及び内側ＮＩＣＩＰアドレスに変換して、ＯＳに備わっているＴＣＰ／ＩＰプロトコルスタック２０５に引き渡す。
なお、宛先ポート番号はそのまま変更しない。
【００２１】
同様に、アドレス変換処理部２０３は、外側ＮＩＣ１０８から受信したパケットに対し、ネットワーク設定情報メモリ２０２、仮ＩＰＭＡＣリスト２０４及び外側ＮＩＣアドレステーブル２１０からそれぞれ情報を読み込み、パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を、第二仮ＮＩＣＭＡＣアドレス、第二仮ＮＩＣＩＰアドレス、索引用ポート番号、外側ＮＩＣＭＡＣアドレス、外側ＮＩＣＩＰアドレス及び動的ポート番号に変換して、ＯＳに備わっているＴＣＰ／ＩＰプロトコルスタック２０５に引き渡す。
【００２２】
また、アドレス変換処理部２０３は、ＴＣＰ／ＩＰプロトコルスタック２０５から外側ＮＩＣ１０８へ送信されるパケットに対し、パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を、索引用ポート番号を手がかりに外側ＮＩＣアドレステーブル２１０を参照して、先に書き換える以前のものに書き戻した後、外側ＮＩＣ１０８から送信する。
【００２３】
同様に、アドレス変換処理部２０３は、ＴＣＰ／ＩＰプロトコルスタック２０５から内側ＮＩＣ１０４へ送信されるパケットに対し、パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を、索引用ポート番号を手がかりに内側ＮＩＣアドレステーブル２０９を参照して、先に書き換える以前のものに書き戻した後、内側ＮＩＣ１０４から送信する。
【００２４】
更に、アドレス変換処理部２０３は、ＴＣＰ／ＩＰプロトコルスタック２０５から外側ＮＩＣ１０８へ送信されるＡＲＰ（Address Resolution Protocol）要求パケットに対し、仮ＩＰＭＡＣリスト２０４に記載されている偽のＭＡＣアドレスで応答することで、あたかも物理媒体から応答があったかのようにＴＣＰ／ＩＰプロトコルスタック２０５を騙して正常に動作させる。
【００２５】
第一のＮＩＣアドレス変換テーブルともいえる内側ＮＩＣアドレステーブル２０９は、アドレス変換処理部２０３が内側ＮＩＣ１０４とＴＣＰ／ＩＰプロトコルスタック２０５との間で、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える、又は書き戻すためのテーブルである。
第二のＮＩＣアドレス変換テーブルともいえる外側ＮＩＣアドレステーブル２１０は、アドレス変換処理部２０３が外側ＮＩＣ１０８とＴＣＰ／ＩＰプロトコルスタック２０５との間で、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える、又は書き戻すためのテーブルである。
これら内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０は、アドレス変換テーブルともいえる。
【００２６】
なお、説明の便宜のため、これ以降、ＸＰＴＣＰ非対応ネットワーク１０９に存在する

ＸＰＴＣＰ非対応ＰＣ１０２、１０３等の、ＸＰＴＣＰに非対応のネットワーク機器を「端末」と称し、ＸＰＴＣＰ対応ネットワーク１１０に存在するＸＰＴＣＰ対応サーバ１０７やＸＰＴＣＰ対応ＰＣ１０６等の、ＸＰＴＣＰに対応しているネットワーク機器を「サーバ」と称する。ＸＰＴＣＰ非対応ＰＣ１０５については、ＸＰＴＣＰを用いた通信の対象外であるので、「端末」「サーバ」の定義からは除外する。

【００２７】

ＴＣＰ／ＩＰプロトコルスタック２０５は、ネットワークＯＳに備わっているネットワークドライバプログラムである。このＴＣＰ／ＩＰプロトコルスタック２０５は、アドレス変換処理部２０３を経由して、ＮＩＣとの間でパケットの送受信を行い、アプリケーションプログラムとの間でデータの送受信を行う。

ＴＣＰ／ＩＰプロトコルスタック２０５はアプリケーションプログラムに対し、周知のソケット（「ＢＳＤソケット」という名称で周知である。）というアプリケーションプログラムインターフェース（ＡＰＩ）を提供する。

ＴＣＰ／ＩＰプロトコルスタック２０５は、ＮＩＣから受信したパケットを、ＡＲＰヘッダ、ＩＰヘッダ、ＴＣＰ又はＵＤＰヘッダの順に除去し、パケットのペイロードを連結してストリームデータに戻し、所定のアプリケーションに引き渡す。

逆に、ＴＣＰ／ＩＰプロトコルスタック２０５は、アプリケーションから受け取ったストリームデータを、ＴＣＰ／ＩＰプロトコルスタック２０５が事前に形成してアプリケーションから指定されたソケットを通じて、所定のデータサイズのペイロードに分割した後、ＴＣＰ又はＵＤＰヘッダ、ＩＰヘッダ、ＡＲＰヘッダの順にヘッダを付加し、ＮＩＣを通じて送信先へ送信する。

【００２８】

特に、ＴＣＰプロトコルのパケットを取り扱う場合には、ＴＣＰ／ＩＰプロトコルスタック２０５は、周知のコネクションという仮想的な通信路を、ＳＹＮ－ＡＣＫ＆ＳＹＮ－ＡＣＫという周知の３ウェイハンドシェイクにてＴＣＰ／ＩＰプロトコルスタック２０５の内部に形成する。

本実施形態のＸＰＴＣＰゲートウェイ装置１０１は、内側ＮＩＣ１０４と外側ＮＩＣ１０８の双方にコネクションを形成し、そのコネクション同士でデータの転送を行う。

【００２９】

内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０は、ＴＣＰ／ＩＰプロトコルスタック２０５が作成するコネクションと、実際のパケットに付されている本来の送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号との関連付けを、索引用ポート番号を設けることで実現している。

内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０は、ＴＣＰ／ＩＰプロトコルスタック２０５が作成するコネクションを管理するテーブルである、ともいえる。

【００３０】

拡張ＴＣＰ処理部ともいえるＸＰＴＣＰ処理部２０６は、ＴＣＰ／ＩＰプロトコルスタック２０５が形成したソケット、すなわち「一方のコネクションの出入口」からデータを受信し、受信したデータをＴＣＰ／ＩＰプロトコルスタック２０５が形成した別のソケット、すなわち「他方のコネクションの出入口」に転送する。

また、ＸＰＴＣＰ処理部２０６はＸＰＴＣＰ処理対象マスタ２０８に記憶されている指示内容に応じて、認証処理及び暗号化通信処理を行う。特にＸＰＴＣＰ処理部２０６は、ＴＣＰ／ＩＰプロトコルスタック２０５から受信したデータを再びＴＣＰ／ＩＰプロトコルスタック２０５に返送する際に、ソケットに付されている送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス、宛先ポート番号を書き換える。

【００３１】

ソケット処理部２０７は、ネットワークＯＳ起動後に自動実行される小さな擬似サーバプログラムであると共に、内側ＮＩＣ１０４から受信したパケットに起因して、ＴＣＰ／

ＩＰプロトコルスタック２０５からｃｏｎｎｅｃｔイベントを受け取ると、ｃｏｎｎｅｃｔイベントを受け取ったソケットに付されている送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス、宛先ポート番号から、外側ＮＩＣ１０８に向けて新たなソケットを作成するためのｃｏｎｎｅｃｔ　ｒｅｑｕｅｓｔイベント、つまり接続要求をＴＣＰ／ＩＰプロトコルスタック２０５に向けて発生する。

ソケット処理部２０７はＴＣＰ／ＩＰプロトコルスタック２０５に対してソケットオープン／クローズ処理のみ行い、ＴＣＰ／ＩＰプロトコルスタック２０５との実際のデータの送受信はＸＰＴＣＰ処理部２０６が行う。

【００３２】

図２に示すＸＰＴＣＰゲートウェイ装置１０１のブロック図のうち、内側ＮＩＣ１０４、外側ＮＩＣ１０８、アドレス変換処理部２０３、ＴＣＰ／ＩＰプロトコルスタック２０５、ＸＰＴＣＰ処理部２０６及びソケット処理部２０７は、周知の７階層のＯＳＩ参照モデルに準拠する、ＴＣＰ／ＩＰの階層モデルに沿っている。

内側ＮＩＣ１０４と外側ＮＩＣ１０８は、ＮＩＣドライバを含めて物理層とデータリンク層に該当する。

ＴＣＰ／ＩＰプロトコルスタック２０５は、ネットワーク層（ＩＰ、ＩＣＭＰ（Internet Control Message Protocol）、ＡＲＰ）とトランスポート層（ＴＣＰ、ＵＤＰ）に該当する。

ソケット処理部２０７はアプリケーション層に該当する。

アドレス変換処理部２０３はデータリンク層とネットワーク層の間に潜り込み、ＴＣＰ／ＩＰプロトコルスタック２０５が本来なら無関係である筈のパケットを処理できるように、パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き換える。このため、アドレス変換処理部２０３はネットワーク層に該当する。

ＸＰＴＣＰ処理部２０６はトランスポート層とアプリケーション層の間に介在して、ソケットオープン／クローズ処理以外の、ネットワークストリームデータの転送と、認証及び暗号化或は復号を行う。このため、ＸＰＴＣＰ処理部２０６はアプリケーション層が介在できない認証及び暗号化通信を実現するトランスポート層に該当すると共に、データを転送するという機能においてアプリケーション層にも該当する。

【００３３】

ネットワークＯＳに標準搭載されているＴＣＰ／ＩＰプロトコルスタック２０５は、本来ならネットワーク設定情報メモリ２０２に記憶されているＩＰアドレス、つまり自らのＮＩＣに付されているＩＰアドレスに対する通信しか取り扱わない。一方、ＸＰＴＣＰゲートウェイ装置１０１はあらゆるパケットを取り扱う必要がある。また、ＸＰＴＣＰは通信の手順が複雑であるＴＣＰ／ＩＰの機能を利用しつつ、トランスポート層における認証と暗号化処理を実現する。

そこで、ＴＣＰ／ＩＰプロトコルスタック２０５の機能を最大限有効に活用しつつ、必要最小限のプログラムを追加することでＸＰＴＣＰゲートウェイ装置１０１を実現するために、本実施形態のＸＰＴＣＰゲートウェイ装置１０１は、ＴＣＰ／ＩＰプロトコルスタック２０５を「騙す」処理を施す。

つまり、ＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレスとは無関係である筈のパケットをＴＣＰ／ＩＰプロトコルスタック２０５が処理できるようにするために、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から受信したパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを、一旦、ＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレス、ＭＡＣアドレス等に書き換える。そして、送信元及び宛先のＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換えた当該パケットをＴＣＰ／ＩＰプロトコルスタック２０５に引き渡す。

アドレス変換処理部２０３及びＸＰＴＣＰ処理部２０６にて行う書換処理、つまりパケットに付されている送信元及び宛先のＭＡＣアドレス、ＩＰアドレスそしてポート番号の

書換処理の詳細は、図１８、図１９及び図２０にて後述する。

【００３４】

［テーブル及びリストの構成］

図３は、ＸＰＴＣＰゲートウェイ装置１０１に備わっている各種テーブル及びリストのフィールド構成を示す図である。

図２に示すＸＰＴＣＰゲートウェイ装置１０１が保有する、内側ＮＩＣアドレステーブル２０９、外側ＮＩＣアドレステーブル２１０、ＸＰＴＣＰポリシーテーブル２１１、仮ＩＰＭＡＣリスト２０４は、図示しないＲＡＭ内に設けられる。また、ＸＰＴＣＰ処理対象マスタ２０８はハードディスク装置等の図示しない不揮発性ストレージに設けられ、アドレス変換処理部２０３が起動する際、図示しないＲＡＭ内に複写される。ネットワーク設定情報メモリ２０２はネットワークＯＳによって図示しないＲＡＭ内に設けられる。

【００３５】

図４はパケットの構造を示す概略図である。内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０のフィールドを、図３のフィールド構成図と図４の概略図を参照して説明する。

内側ＮＩＣアドレステーブル２０９は、プロトコル種別フィールドと、送信元ＭＡＣアドレスフィールドと、送信元ＩＰアドレスフィールドと、送信元ポート番号フィールドと、宛先ＭＡＣアドレスフィールドと、宛先ＩＰアドレスフィールドと、宛先ポート番号フィールドと、索引用ポート番号フィールドと、タイマ用カウンタ値フィールドを有する。

外側ＮＩＣアドレステーブル２１０は、プロトコル種別フィールドと、送信元ＭＡＣアドレスフィールドと、送信元ＩＰアドレスフィールドと、送信元ポート番号フィールドと、宛先ＭＡＣアドレスフィールドと、宛先ＩＰアドレスフィールドと、宛先ポート番号フィールドと、索引用ポート番号フィールドと、動的ポート番号フィールドと、タイマ用カウンタ値フィールドを有する。

【００３６】

プロトコル種別フィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットの種別として、ＴＣＰ又はＵＤＰを示すフラグが格納される。これはＩＰヘッダ４０１のプロトコル番号から読み取る。なお、本実施形態のＸＰＴＣＰゲートウェイ装置１０１は、現段階ではＴＣＰパケットのみを扱うが、近い将来にＵＤＰパケットを処理可能にするために、このプロトコル種別フィールドが用意されている。

送信元ＭＡＣアドレスフィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットに付されている送信元ＭＡＣアドレスが格納される。これはＭＡＣヘッダ４０２の送信元ＭＡＣアドレスから読み取る。

送信元ＩＰアドレスフィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットに付されている送信元ＩＰアドレスが格納される。これはＩＰヘッダ４０１の送信元ＩＰアドレスから読み取る。

送信元ポート番号フィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットに付されている送信元ポート番号が格納される。これはＴＣＰヘッダ４０３又はＵＤＰヘッダ４０４の送信元ポート番号から読み取る。

宛先ＭＡＣアドレスフィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットに付されている宛先ＭＡＣアドレスが格納される。これはＭＡＣヘッダ４０２の宛先ＭＡＣアドレスから読み取る。

宛先ＩＰアドレスフィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットに付されている宛先ＩＰアドレスが格納される。これはＩＰヘッダ４０１の宛先ＩＰアドレスから読み取る。

宛先ポート番号フィールドには、内側ＮＩＣ１０４又は外側ＮＩＣ１０８から入って来るパケットに付されている宛先ポート番号が格納される。これはＴＣＰヘッダ４０３又はＵＤＰヘッダ４０４の宛先ポート番号から読み取る。

【００３７】

索引用ポート番号フィールドには、アドレス変換処理部２０３がパケットを内側ＮＩＣ

１０４又は外側ＮＩＣ１０８から送信する直前に、パケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き戻す際に、内側ＮＩＣアドレステーブル２０９又は外側ＮＩＣアドレステーブル２１０のどのレコードに記述されているかを特定するための索引情報が格納される。

この索引用ポート番号は、ＸＰＴＣＰ処理対象マスタ２０８のレコードに処理対象として合致するＴＣＰ　ＳＹＮパケットが内側ＮＩＣ１０４から来た時に、アドレス変換処理部２０３が内側ＮＩＣアドレステーブル２０９に新規レコードを追記録する際、図２のＴＣＰポート番号メモリ２１２の値が用いられる。索引用ポート番号は、ポート番号を索引情報として利用するので、一意性（ユニークであり、重複しない）を有することが求められる。このため、ＴＣＰポート番号メモリ２１２の値を利用とした際に、既に当該番号が使われている場合は、ＴＣＰポート番号メモリ２１２の値をインクリメントして、当該ポート番号が空いているか、確認する。

【００３８】

ＴＣＰ　ＳＹＮパケットとは、周知のＴＣＰ通信の開始（コネクションの確立要求）を表すパケットであり、ＴＣＰヘッダ４０３に存在する６ビットのコードビットの５番目のビットが「１」のパケットである。

ＴＣＰ　ＡＣＫパケットとは、周知のＴＣＰ通信における確認応答を表すパケットであり、ＴＣＰヘッダ４０３に存在する６ビットのコードビットの２番目のビットが「１」のパケットである。

ＴＣＰ　ＦＩＮパケットとは、周知のＴＣＰ通信の終了（コネクションの切断要求）を表すパケットであり、ＴＣＰヘッダ４０３に存在する６ビットのコードビットの６番目のビットが「１」のパケットである。

ＴＣＰ　ＡＣＫ／ＳＹＮパケットとは、ＴＣＰヘッダ４０３に存在する６ビットのコードビットの２番目のビットと５番目のビットが「１」のパケットであり、ＴＣＰ　ＳＹＮパケットとＴＣＰ　ＡＣＫパケットの、二つの意味を同時に備えている。

【００３９】

外側ＮＩＣアドレステーブル２１０にのみ設けられている動的ポート番号は、動的ポート番号フィールドに格納される。この動的ポート番号は、ＴＣＰ／ＩＰプロトコルスタック２０５が外側ＮＩＣ１０８を通じて、ＸＰＴＣＰ対応ネットワーク１１０に存在するＸＰＴＣＰ対応サーバ１０７やＸＰＴＣＰ対応ＰＣ１０６等の、ＸＰＴＣＰに対応しているネットワーク機器、すなわちサーバとのコネクションを形成する際、当該コネクションの送信元ポート番号として、ＴＣＰ／ＩＰプロトコルスタック２０５が自動的に生成するポート番号である。多くの場合、動的ポート番号は「短命なポート」とも呼ばれる周知のエフェメラルポートの番号である、ポート番号４９１５２から６５５３５迄の番号が、ＴＣＰ／ＩＰプロトコルスタック２０５によって付与される。

【００４０】

タイマ用カウンタ値フィールドには、内側ＮＩＣアドレステーブル２０９又は外側ＮＩＣアドレステーブル２１０の当該レコードが利用されなくなったことを判断して破棄する際の、経過時間を計測する為のアドレステーブル更新カウンタ２１３の値が格納される。

【００４１】

図３に示すネットワーク設定情報メモリ２０２には、ネットワークＯＳが起動する際にネットワークの基本設定を行った結果の、内側ＮＩＣ１０４及び外側ＮＩＣ１０８のＭＡＣアドレス及びＩＰアドレスが記憶される。つまり、ネットワーク設定情報メモリ２０２はネットワークＯＳによって設けられる。

内側ＮＩＣＭＡＣアドレスは、内側ＮＩＣ１０４の、本来のＭＡＣアドレスを示す。

内側ＮＩＣＩＰアドレスは、内側ＮＩＣ１０４の、本来のＩＰアドレスを示す。

外側ＮＩＣＭＡＣアドレスは、外側ＮＩＣ１０８の、本来のＭＡＣアドレスを示す。

外側ＮＩＣＩＰアドレスは、外側ＮＩＣ１０８の、本来のＩＰアドレスを示す。

【００４２】

同じく図３に示す仮ＩＰＭＡＣリスト２０４は、内側ＮＩＣＩＰアドレスフィールドと、第一仮ＭＡＣアドレスフィールドと、第一仮ＩＰアドレスフィールドと、外側ＮＩＣＩＰアドレスフィールドと、第二仮ＭＡＣアドレスフィールドと、第二仮ＩＰアドレスフィールドを有する。

内側ＮＩＣＩＰアドレスフィールドには、内側ＮＩＣ１０４のＩＰアドレスが格納される。これはネットワーク設定情報メモリ２０２から得られる。

第一仮ＭＡＣアドレスフィールドには、第一仮ＭＡＣアドレスが格納される。

第一仮ＩＰアドレスフィールドには、第一仮ＩＰアドレスが格納される。

外側ＮＩＣＩＰアドレスフィールドには、外側ＮＩＣ１０８のＩＰアドレスが格納される。これはネットワーク設定情報メモリ２０２から得られる。

第二仮ＭＡＣアドレスフィールドには、第二仮ＭＡＣアドレスが格納される。

第二仮ＩＰアドレスフィールドには、第二仮ＩＰアドレスが格納される。

第一仮ＭＡＣアドレス、第一仮ＩＰアドレス、第二仮ＭＡＣアドレス及び第二仮ＩＰアドレスは、アドレス変換処理部２０３及びＸＰＴＣＰ処理部２０６にて用いる、偽のＭＡＣアドレス及びＩＰアドレスである。

【００４３】

同じく拡張ＴＣＰ処理対象マスタともいえる、図３に示すＸＰＴＣＰ処理対象マスタ２０８は、レコード番号フィールドと、プロトコル種別フィールドと、送信元ＩＰアドレスフィールドと、送信元ポート番号フィールドと、宛先ＩＰアドレスフィールドと、宛先ポート番号フィールドと、暗号種別他フィールドを有する。

レコード番号フィールドは、ＸＰＴＣＰ処理対象マスタ２０８のレコード番号そのものである。ＸＰＴＣＰ処理対象マスタ２０８のレコードを一意に識別する連番の番号である。なお、レコード番号フィールドに格納する情報は、後述するＸＰＴＣＰポリシーテーブル２１１にて用いる、レコードを一意に識別するための情報である。したがって、一意に識別が可能であれば、必ずしもレコード番号でなくても良い。

プロトコル種別フィールドには、内側ＮＩＣ１０４から入って来るパケットの種別として、ＴＣＰ又はＵＤＰを示すフラグが格納される。これはＩＰヘッダ４０１のプロトコル番号から読み取る。

送信元ＩＰアドレスフィールドには、内側ＮＩＣ１０４から入って来るパケットに付されている送信元ＩＰアドレスが格納される。これはＩＰヘッダ４０１の送信元ＩＰアドレスから読み取る。

送信元ポート番号フィールドには、内側ＮＩＣ１０４から入って来るパケットに付されている送信元ポート番号が格納される。これはＴＣＰヘッダ４０３又はＵＤＰヘッダ４０４の送信元ポート番号から読み取る。

宛先ＩＰアドレスフィールドには、内側ＮＩＣ１０４から入って来るパケットに付されている宛先ＩＰアドレスが格納される。これはＩＰヘッダ４０１の宛先ＩＰアドレスから読み取る。

宛先ポート番号フィールドには、内側ＮＩＣ１０４から入って来るパケットに付されている宛先ポート番号が格納される。これはＴＣＰヘッダ４０３又はＵＤＰヘッダ４０４の宛先ポート番号から読み取る。

暗号種別他フィールドには、当該ＸＰＴＣＰセッションに用いる認証や暗号の種類等の情報が格納される。

つまり、ＸＰＴＣＰ処理対象マスタ２０８には、端末からサーバに向けて送信されるパケットのＩＰアドレス及びポート番号の組み合わせと、そのＩＰアドレス及びポート番号の組み合わせを有するパケットによって、内側ＮＩＣ１０４及び外側ＮＩＣ１０８の夫々に形成されるコネクションを通過するデータストリームに適用する、暗号化等に関する情報が記憶される。

【００４４】

同じく図３に示すＸＰＴＣＰポリシーテーブル２１１は、プロトコル種別フィールドと、索引用ポート番号フィールドと、レコード番号フィールドを有する。

プロトコル種別フィールドには、ＸＰＴＣＰ処理対象マスタ２０８と同様、内側ＮＩＣ１０４から入って来るパケットの種別として、ＴＣＰ又はＵＤＰを示すフラグが格納される。これはＩＰヘッダ４０１のプロトコル番号から読み取る。

索引用ポート番号フィールドには、当該セッションのパケットに対してアドレス変換処理部２０３によって付されている、索引用ポート番号が格納される。

レコード番号フィールドは、ＸＰＴＣＰ処理対象マスタ２０８のレコード番号そのものである。したがって、このフィールドに記されているレコード番号で、ＸＰＴＣＰ処理対象マスタ２０８のレコードを指定し、当該レコードの暗号種別他フィールドを参照する。

ＸＰＴＣＰポリシーテーブル２１１は、索引用ポート番号と暗号種別他の情報を紐付けることで、索引用ポート番号に係るＴＣＰコネクションを通過するデータストリームに適用する、暗号種別等を特定する。

【００４５】

再び図２に戻って、各部の説明を続ける。

アドレステーブル更新カウンタ２１３は、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の、使われなくなったレコードを削除する際に、経過時間を見るためのカウンタである。アドレステーブル更新カウンタ２１３は、一例としては０から１１９迄の数を計数するループカウンタである。０から始まり、１秒毎に計数値が１インクリメントして、１１９迄計数すると、再度０から計数を開始する。

アドレス変換処理部２０３は、後述するＴＣＰ切断シーケンスにおいて、ＴＣＰ　ＦＩＮパケットが内側ＮＩＣ１０４及び外側ＮＩＣ１０８の両方から来たことに呼応して、アドレステーブル更新カウンタ２１３の値を、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の該当するレコードの、タイマ用カウント値フィールドに書き込む。そして、タイマ用カウント値フィールドの値と現在のアドレステーブル更新カウンタ２１３の値を比較して、６０秒以上を経過したと判断したら、もはやそのレコードに示される通信セッションは終了したと判断して、当該レコードを削除する。

【００４６】

ＴＣＰポート番号メモリ２１２は、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の索引用ポート番号フィールドに値を記入するためのポート番号が格納されるメモリである。

内側ＮＩＣ１０４からＴＣＰ　ＳＹＮパケットが来ると、新たなコネクションを作成する必要がある。アドレス変換処理部２０３はＴＣＰ／ＩＰプロトコルスタック２０５にコネクションを作成させるために、アドレス変換処理を行う。アドレス変換処理によって、ＴＣＰ／ＩＰプロトコルスタック２０５は本来の送信元ＩＰアドレス及び宛先ＩＰアドレス等とは異なる、偽の送信元ＩＰアドレス及び宛先ＩＰアドレス等が付されたパケットに対して、コネクションを形成する。

【００４７】

アドレス変換処理部２０３は、偽の送信元ＩＰアドレス及び宛先ＩＰアドレス等をパケットに付する際、ＴＣＰ／ＩＰプロトコルスタック２０５が作成するコネクションと、その偽の送信元ＩＰアドレス及び宛先ＩＰアドレス等との関連付けを行わなければならない。このコネクションを識別して、最終的に本来の送信元ＩＰアドレス及び宛先ＩＰアドレス等に戻すために、パケットに識別情報を付する必要がある。これが、索引用ポート番号である。

内側ＮＩＣアドレステーブル２０９に新たなレコードが作成された際、ＴＣＰポート番号メモリ２１２の値を１インクリメントして、その値を索引用ポート番号フィールドに書き込む。

索引用ポート番号はＴＣＰ／ＩＰプロトコルスタック２０５が認識可能な番号でなければならないので、ＴＣＰポート番号メモリ２１２に記入される最大値は６５５３５である。

ＴＣＰポート番号メモリ２１２は、「短命なポート」とも呼ばれる周知のエフェメラルポートの番号である、ポート番号４９１５２から６５５３５迄を１ずつインクリメントす

る値が書き込まれる。なお、ＴＣＰポート番号メモリ２１２はループカウンタで構成しても良い。

【００４８】

［アドレス変換処理部２０３の内部構成］

図５は、アドレス変換処理部２０３の機能ブロック図である。

アドレス変換処理部２０３は、内側ＮＩＣ受信処理部５０１、外側ＮＩＣ受信処理部５０２、外側ＮＩＣ送信処理部５０３、内側ＮＩＣ送信処理部５０４、テーブル更新処理部５０５、及びポリシー回答部５０６の、五つの機能ブロックに分けられる。

【００４９】

先ず、内側ＮＩＣ受信処理部５０１の詳細を説明する。図６は、内側ＮＩＣ受信処理部５０１の機能ブロック図である。

内側ＮＩＣ１０４が受信したパケットは、最初に受信パケット判定部６０１がＸＰＴＣＰ処理対象マスタ２０８を参照して、当該パケットがＸＰＴＣＰ処理の対象になるか否か等を判定する。

もし、内側ＮＩＣ１０４が受信したパケットが、例えばＩＣＭＰパケットやＸＰＴＣＰ処理対象マスタ２０８に合致しない処理対象外パケットである場合は、受信パケット判定部６０１はそのパケットをそのまま外側ＮＩＣ１０８へ転送する。

もし、内側ＮＩＣ１０４が受信したパケットが、ＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットである場合は、受信パケット判定部６０１はそのパケットをそのままＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。

もし、内側ＮＩＣ１０４から入力されたパケットがＸＰＴＣＰ処理対象マスタ２０８に合致する処理対象パケットである場合は、受信パケット判定部６０１は次にそのパケットの詳細を見る。

【００５０】

受信パケット判定部６０１は、そのパケットがＴＣＰデータパケットであれば、当該ＴＣＰデータパケットをアドレス置換部６０２に引き渡す。

アドレス置換部６０２は内側ＮＩＣアドレステーブル２０９を送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号で検索して、レコードを特定し、パケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換えて、ＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。

【００５１】

受信パケット判定部６０１で処理するパケットがＴＣＰ　ＳＹＮパケットであれば、それは内側ＮＩＣアドレステーブル２０９に未登録のパケットである。そこで、受信パケット判定部６０１はＴＣＰ　ＳＹＮパケットをコネクション登録処理部６０３に引き渡す。コネクション登録処理部６０３は、ＴＣＰ　ＳＹＮパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号で、内側ＮＩＣアドレステーブル２０９に新規のレコードを追記録する。そして、ＴＣＰポート番号メモリ２１２の値を１インクリメントして参照し、その値を索引用ポート番号として内側ＮＩＣアドレステーブル２０９の索引用ポート番号フィールドに記録する。更に、同じ内容のレコードを外側ＮＩＣアドレステーブル２１０にも追記録する。その後、コネクション登録処理部６０３はＴＣＰ　ＳＹＮパケットをアドレス置換部６０２に引き渡す。アドレス置換部６０２は前述のＴＣＰデータパケットと同様に、ＴＣＰ　ＳＹＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換えて、ＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。

【００５２】

受信パケット判定部６０１で処理するパケットがＴＣＰ　ＦＩＮパケットであれば、それはＴＣＰ／ＩＰプロトコルスタック２０５に形成されたコネクションの終了を意味すると共に、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の該

当レコードを削除する必要が生じる。但し、レコードを削除する時期は、内側ＮＩＣ１０４に向けて形成されているコネクションと、外側ＮＩＣ１０８に向けて形成されているコネクションとの、両方のコネクションの終了から所定の時間を経過させる必要がある。

そこで、受信パケット判定部６０１はＴＣＰ　ＦＩＮパケットをレコード削除準備処理部６０４に引き渡す。

レコード削除準備処理部６０４は、ＴＣＰ　ＦＩＮパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号で内側ＮＩＣアドレステーブルを検索してレコードを特定し、当該レコードの索引ポート番号を削除予定リスト６０５に書き出す。削除予定リスト６０５は、図示しないＲＡＭ内に設けられた、削除を予定しているレコードの索引ポート番号が記録されるリストである。その後、レコード削除準備処理部６０４はＴＣＰ　ＦＩＮパケットをアドレス置換部６０２に引き渡す。アドレス置換部６０２は前述のＴＣＰデータパケット及びＴＣＰ　ＳＹＮパケットと同様に、ＴＣＰ　ＦＩＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換えて、ＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。

【００５３】

なお、アドレス置換部６０２は、ＴＣＰデータパケット、ＴＣＰ　ＳＹＮパケット及びＴＣＰ　ＦＩＮパケットの何れの場合においても宛先ポート番号は書き換えない。

アドレス置換部６０２は、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える際、仮ＩＰＭＡＣリスト２０４を参照する。

【００５４】

次に、外側ＮＩＣ受信処理部５０２の詳細を説明する。

図７は、外側ＮＩＣ受信処理部５０２の機能ブロック図である。

外側ＮＩＣ１０８が受信したパケットは、最初に受信パケット判定部７０１がＸＰＴＣＰ処理対象マスタ２０８を参照して、当該パケットがＸＰＴＣＰ処理の対象になるか否か等を判定する。

もし、外側ＮＩＣ１０８が受信したパケットが、例えばＩＣＭＰパケットやＸＰＴＣＰ処理対象マスタ２０８に合致しない処理対象外パケットである場合は、外側ＮＩＣ受信処理部５０２はそのパケットをそのまま内側ＮＩＣ１０４へ転送する。

もし、外側ＮＩＣ１０８が受信したパケットが、ＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットである場合は、外側ＮＩＣ受信処理部５０２はそのパケットをそのままＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。

もし、外側ＮＩＣ１０８から入力されたパケットがＸＰＴＣＰ処理対象マスタ２０８に合致する処理対象パケットである場合は、受信パケット判定部７０１は次にそのパケットの詳細を見る。

【００５５】

受信パケット判定部７０１は、そのパケットがＴＣＰデータパケットであれば、当該ＴＣＰデータパケットをアドレス置換部７０２に引き渡す。

アドレス置換部７０２は外側ＮＩＣアドレステーブル２１０を送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号で検索してレコードを特定し、パケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き換えて、ＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。

【００５６】

受信パケット判定部７０１は、もし、そのパケットがＴＣＰ　ＦＩＮパケットであれば、それはＴＣＰ／ＩＰプロトコルスタック２０５に形成されたコネクションの終了を意味すると共に、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の該当レコードを削除する必要が生じる。前述のように、レコードを削除する時期は、外側ＮＩＣ１０８に向けて形成されているコネクションと、外側ＮＩＣ１０８に向けて形成されているコネクションとの、両方のコネクションの終了から所定の時間を経過させる必

要がある。
そこで、受信パケット判定部７０１はＴＣＰ　ＦＩＮパケットをレコード削除処理部７０３に引き渡す。
レコード削除処理部７０３は、ＴＣＰ　ＦＩＮパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号で内側ＮＩＣアドレステーブルを検索してレコードを特定し、当該レコードの索引ポート番号を取得する。
次に、取得した索引ポート番号が削除予定リスト６０５にあるか否かを確認する。削除予定リスト６０５に当該索引ポート番号があったなら、現時点のアドレステーブル更新カウンタ２１３の値を、当該索引ポート番号に係る外側ＮＩＣアドレステーブル２１０及び内側ＮＩＣアドレステーブル２０９のレコードの、タイマ用カウンタ値フィールドに書き込む。その後、レコード削除処理部７０３はＴＣＰ　ＦＩＮパケットをアドレス置換部７０２に引き渡す。
アドレス置換部７０２は前述のＴＣＰデータパケットと同様に、ＴＣＰ　ＦＩＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス宛先ＩＰアドレス及び宛先ポート番号を書き換えて、ＴＣＰ／ＩＰプロトコルスタック２０５へ転送する。
アドレス置換部７０２は、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える際、仮ＩＰＭＡＣリスト２０４を参照する。

【００５７】

次に、外側ＮＩＣ送信処理部５０３の詳細を説明する。
図８は、外側ＮＩＣ送信処理部５０３の機能ブロック図である。
送信パケット判定部８０１は、ＴＣＰ／ＩＰプロトコルスタック２０５から送出されたパケットを受信すると、最初にパケットがアドレス書換対象外パケットか、アドレス書換対象ＴＣＰパケットか、或はＡＲＰ要求パケットかを判定する。
もし、パケットがアドレス書換対象外のパケットであれば、そのまま何もせずに外側ＮＩＣ１０８に送信する。

【００５８】

もし、パケットがＡＲＰ要求パケットであり、且つＡＲＰ要求パケットに付されている問い合わせＩＰアドレスが第二仮ＩＰアドレスである場合は、当該パケットは、パケットに付するＭＡＣアドレスを特定するために、ＴＣＰ／ＩＰプロトコルスタック２０５がコネクションを形成する際に送信するパケットである。そこで、送信パケット判定部８０１はＡＲＰ要求パケットをＡＲＰ応答処理部８０２に引き渡す。
ＡＲＰ応答処理部８０２は仮ＩＰＭＡＣリスト２０４を参照して、ＴＣＰ／ＩＰプロトコルスタック２０５に第二仮ＭＡＣアドレスを返答する。

【００５９】

もし、パケットがＴＣＰパケットであり、パケットに付されている宛先ＩＰアドレスが第二仮ＩＰアドレスである場合は、送信パケット判定部８０１は次に当該パケットがＴＣＰ　ＳＹＮパケットであるか否かを確認する。ＴＣＰ　ＳＹＮパケットであれば、それはＴＣＰ／ＩＰプロトコルスタック２０５がコネクションを新規に作成したことを示す。したがって、ＴＣＰ／ＩＰプロトコルスタック２０５が新規に作成したコネクションの送信元ポート番号、つまり動的ポート番号を、外側ＮＩＣアドレステーブル２１０に記憶しておく必要がある。そこで、送信パケット判定部８０１はＴＣＰ ＳＹＮパケットを動的ポート記録処理部８０３に引き渡す。
動的ポート記録処理部８０３は、ＴＣＰ　ＳＹＮパケットに付されている送信元ポート番号、つまり動的ポート番号と、宛先ポート番号として付されている索引ポート番号を取得する。そして、索引ポート番号で外側ＮＩＣアドレステーブル２１０の該当レコードを特定したら、当該レコードの動的ポート番号フィールドに、動的ポート番号を記録する。そして、動的ポート記録処理部８０３は当該ＴＣＰ ＳＹＮパケットをアドレス復元部８０４に引き渡す。

アドレス復元部８０４は外側ＮＩＣアドレステーブル２１０の、先に宛先ポート番号で特定したレコードの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を取得し、パケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き戻して、外側ＮＩＣ１０８に送信する。

【００６０】

もし、パケットがＴＣＰパケットであり、パケットに付されている宛先ＩＰアドレスが第二仮ＩＰアドレスである場合は、送信パケット判定部８０１は次に当該パケットがＴＣＰ　ＳＹＮパケットであるか否かを確認する。ＴＣＰ　ＳＹＮパケットでなければ、送信パケット判定部８０１は当該ＴＣＰパケットをアドレス復元部８０４に引き渡す。

アドレス復元部８０４は外側ＮＩＣアドレステーブル２１０の、先に索引ポート番号で特定したレコードの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を取得し、パケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き戻して、外側ＮＩＣ１０８に送信する。

【００６１】

次に、内側ＮＩＣ送信処理部５０４の詳細を説明する。

図９は、内側ＮＩＣ送信処理部５０４の機能ブロック図である。

送信パケット判定部９０１は、ＴＣＰ／ＩＰプロトコルスタック２０５から送出されたパケットを受信すると、最初にパケットがアドレス書換対象外パケットか、或はアドレス書換対象ＴＣＰパケットかを判定する。

もし、パケットがアドレス書換対象外のパケットであれば、そのまま何もせずに内側ＮＩＣ１０４に送信する。

もし、パケットがＴＣＰパケットであり、パケットに付されている宛先ＩＰアドレスが第一仮ＩＰアドレスである場合は、送信パケット判定部９０１は当該ＴＣＰパケットをアドレス復元部９０２に引き渡す。

アドレス復元部９０２は内側ＮＩＣアドレステーブル２０９の、索引ポート番号で特定したレコードの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を取得し、パケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き戻して、内側ＮＩＣ１０４に送信する。

【００６２】

次に、テーブル更新処理部５０５の詳細を説明する。

テーブル更新処理部５０５は１秒毎に起動し、アドレステーブル更新カウンタ２１３の値を１インクリメントして、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の全てのレコードのタイマ用カウント値フィールドを検査し、ＴＣＰ　ＦＩＮパケットが来てクローズされたコネクションが６０秒以上経過したレコードがあるか否かを確認する。そして、そのようなレコードがあれば当該レコードを削除する。

【００６３】

次に、ポリシー回答部５０６の詳細を説明する。

ポリシー回答部５０６は、ＸＰＴＣＰ処理部２０６から送出される、索引ポート番号を伴うポリシー問い合わせに対し、ＸＰＴＣＰ処理対象マスタ２０８及び内側ＮＩＣアドレステーブル２０９を参照して、当該索引ポート番号で特定されるコネクションに対する暗号種別等を指定するための、ＸＰＴＣＰ処理対象マスタ２０８のレコード番号を返答する。

【００６４】

［ＸＰＴＣＰ処理部２０６の内部構成］

図１０は、ＸＰＴＣＰ処理部２０６の機能ブロック図である。

イベント検出部１００１は、ＴＣＰ／ＩＰプロトコルスタック２０５から得られる、ａｃｃｅｐｔイベント、ｃｏｎｎｅｃｔ　ｒｅｑｕｅｓｔイベント及びｃｌｏｓｅイベント

を検出し、ソケット操作部１００２及びポリシー設定部１００３を制御する。
ソケット操作部１００２は、ＴＣＰ／ＩＰプロトコルスタック２０５によって図示しないＲＡＭ上に形成されたソケットメモリ領域１００４に対し、ソケットから得られるストリームデータを、暗号化処理部１００５又は復号処理部１００６に引き渡し、処理されたストリームデータをソケットメモリ領域１００４上の所定のソケットに引き渡す。
ポリシー設定部１００３は、ソケット操作部１００２からイベント検出部１００１を通じて得られた索引ポート番号を引数として、アドレス変換処理部に対してポリシーを問い合わせる。この問い合わせに対しては、アドレス変換処理部のポリシー回答部５０６がＸＰＴＣＰ処理対象マスタ２０８のレコード番号を返答する。すると、ポリシー設定部１００３はＸＰＴＣＰポリシーテーブル２１１に、索引ポート番号とＸＰＴＣＰ処理対象マスタ２０８のレコード番号を記録して、紐付ける。
暗号化処理部１００５は、ＸＰＴＣＰポリシーテーブル２１１及びＸＰＴＣＰ処理対象マスタ２０８を参照して、ソケット操作部１００２から受け取ったストリームデータに対して、指定された暗号化処理を遂行する。
復号処理部１００６は、ＸＰＴＣＰポリシーテーブル２１１及びＸＰＴＣＰ処理対象マスタ２０８を参照して、ソケット操作部１００２から受け取ったストリームデータに対して、指定された復号処理を遂行する。
なお、本来ならＸＰＴＣＰ処理部２０６には、認証に関する機能も存在するが、本実施形態のＸＰＴＣＰゲートウェイ装置１０１では、認証に関する動作は発明の範疇から外れるので、敢えて認証に関する記述は省略している。このため、図１０に示すＸＰＴＣＰ処理部２０６の機能ブロック図には、認証に関する機能ブロックは記述を省略している。

【００６５】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・アドレス変換処理部２０３の動作］

これより、図１１から図１７のフローチャートに基づいて、ＸＰＴＣＰゲートウェイ装置１０１の動作の流れを説明する。

【００６６】

図１１は、アドレス変換処理部２０３の、内側ＮＩＣ１０４におけるパケット受信処理の動作の流れを示すフローチャートである。これは内側ＮＩＣ受信処理部５０１の動作の流れに該当する。
処理を開始すると（Ｓ１１０１）、受信パケット判定部６０１は、最初に内側ＮＩＣ１０４が受信したパケットが、例えばＡＲＰパケットやＩＣＭＰパケット等の、明らかに転送対象となる処理対象外パケットであるか否かを判定する（Ｓ１１０２）。
判定の結果、受信したパケットが、ＡＲＰパケットやＩＣＭＰパケット等の、明らかに転送対象となる処理対象外パケットである場合は（Ｓ１１０２のＹＥＳ）、受信パケット判定部６０１はそのパケットをそのまま外側ＮＩＣ１０８へ転送して（Ｓ１１０３）、一連の処理を終了する（Ｓ１１０４）。

【００６７】

ステップＳ１１０２において、受信したパケットが、明らかに転送対象となる処理対象外パケットでない場合（Ｓ１１０２のＮＯ）は、受信パケット判定部６０１は次にそのパケットがＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットであるか否かを判定する（Ｓ１１０５）。
判定の結果、受信したパケットが、ＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットである場合は（Ｓ１１０５のＹＥＳ）、受信パケット判定部６０１はそのパケットをそのままＴＣＰ／ＩＰプロトコルスタック２０５へ転送して（Ｓ１１０６）、一連の処理を終了する（Ｓ１１０４）。

【００６８】

ステップＳ１１０５において、受信したパケットが、ＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットでない場合は（Ｓ１１０５のＮＯ）、受信パケット判定部６０１は次に当該パケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号でＸＰＴＣＰ処理対象マスタ２０８を検索す

る（Ｓ１１０７）。
検索の結果、受信したパケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号の組み合わせが、ＸＰＴＣＰ処理対象マスタ２０８になければ（Ｓ１１０８のＮＯ）、当該パケットはＸＰＴＣＰゲートウェイ装置１０１の処理対象外なので、受信パケット判定部６０１はそのパケットをそのまま外側ＮＩＣ１０８へ転送して（Ｓ１１０３）、一連の処理を終了する（Ｓ１１０４）。

【００６９】
ステップＳ１１０８において、受信したパケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号の組み合わせが、ＸＰＴＣＰ処理対象マスタ２０８にあれば（Ｓ１１０８のＹＥＳ）、当該パケットはＸＰＴＣＰゲートウェイ装置１０１の処理対象であり、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える必要がある。そこで、受信パケット判定部６０１は更に受信したパケットの詳細を見る。
受信パケット判定部６０１は、受信したパケットがＴＣＰ　ＳＹＮパケットであるか否かを判定する（Ｓ１１０９）。
判定の結果、受信したパケットがＴＣＰ　ＳＹＮパケットであれば（Ｓ１１０９のＹＥＳ）、受信パケット判定部６０１は当該ＴＣＰ　ＳＹＮパケットをコネクション登録処理部６０３に引き渡す。
コネクション登録処理部６０３は、ＴＣＰ　ＳＹＮパケットを受け取ると、ＴＣＰポート番号メモリを参照して、現時点で使われていない（重複しない）新たな索引ポート番号を得た後、受信したパケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号と共に、内側ＮＩＣアドレステーブル２０９に新規のレコードとして追記録する（Ｓ１１１０）。更に、同じ内容で外側ＮＩＣアドレステーブル２１０にも同様に新規レコードを追記録する（Ｓ１１１１）。

【００７０】
コネクション登録処理部６０３は、内側ＮＩＣアドレステーブル２０９と外側ＮＩＣアドレステーブル２１０に新規レコードを追記録した後、受信パケット判定部６０１から引き渡されたＴＣＰ　ＳＹＮパケットをアドレス置換部６０２に引き渡す。

【００７１】
アドレス置換部６０２は、コネクション登録処理部６０３から引き渡された索引ポート番号と仮ＩＰＭＡＣリスト２０４を参照して、ＴＣＰ　ＳＹＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換える（Ｓ１１１２）。具体的には、
・パケットに付されている送信元ＭＡＣアドレスを第一仮ＭＡＣアドレスに、
・パケットに付されている送信元ＩＰアドレスを第一仮ＩＰアドレスに、
・パケットに付されている送信元ポート番号を索引ポート番号に、
・パケットに付されている宛先ＭＡＣアドレスを内側ＮＩＣＭＡＣアドレスに、
・パケットに付されている宛先ＩＰアドレスを内側ＮＩＣＩＰアドレスに書き換える。
そして、宛先ポート番号は変更しない。
アドレス置換部６０２はＩＰアドレス等の置換処理を行った後、当該ＴＣＰ　ＳＹＮパケットをＴＣＰ／ＩＰプロトコルスタック２０５に送信して（Ｓ１１０６）、一連の処理を終了する（Ｓ１１０４）。

【００７２】
ステップＳ１１０９において、受信したパケットがＴＣＰ　ＳＹＮパケットでなければ（Ｓ１１０９のＮＯ）、受信パケット判定部６０１は次に受信したパケットがＴＣＰ　ＦＩＮパケットであるか否かを判定する（Ｓ１１１３）。
判定の結果、受信したパケットがＴＣＰ　ＦＩＮパケットであれば（Ｓ１１０９のＹＥＳ）、受信パケット判定部６０１は当該ＴＣＰ　ＦＩＮパケットを索引ポート番号と共にレコード削除準備処理部６０４に引き渡す。
レコード削除準備処理部６０４は、当該ＴＣＰ　ＦＩＮパケットの索引ポート番号を削

除予定リスト６０５に書き込む（Ｓ１１０４）。その後、レコード削除準備処理部６０４はＴＣＰ　ＦＩＮパケットと索引ポート番号をアドレス置換部６０２に引き渡す。

【００７３】

アドレス置換部６０２は、受信パケット判定部６０１からレコード削除準備処理部６０４を通じて引き渡された索引ポート番号と仮ＩＰＭＡＣリスト２０４を参照して、ＴＣＰ　ＦＩＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換える（Ｓ１１１２）。具体的には、パケットに付されている送信元ＭＡＣアドレスを第一仮ＭＡＣアドレスに、パケットに付されている送信元ＩＰアドレスを第一仮ＩＰアドレスに、パケットに付されている送信元ポート番号を索引ポート番号に、パケットに付されている宛先ＭＡＣアドレスを内側ＮＩＣＭＡＣアドレスに、パケットに付されている宛先ＩＰアドレスを内側ＮＩＣＩＰアドレスに書き換える。そして、宛先ポート番号は変更しない。

アドレス置換部６０２はＩＰアドレス等の置換処理を行った後、当該ＴＣＰ　ＦＩＮパケットをＴＣＰ／ＩＰプロトコルスタック２０５に送信して（Ｓ１１０６）、一連の処理を終了する（Ｓ１１０４）。

【００７４】

ステップＳ１１１３において、受信したパケットがＴＣＰ　ＦＩＮパケットでなければ（Ｓ１１１３のＮＯ）、当該パケットはＴＣＰデータパケットである。そこで、受信パケット判定部６０１は当該ＴＣＰデータパケットを索引ポート番号と共にアドレス置換部６０２に引き渡す。

【００７５】

アドレス置換部６０２は、受信パケット判定部６０１から引き渡された索引ポート番号と仮ＩＰＭＡＣリスト２０４を参照して、ＴＣＰデータパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換える（Ｓ１１１２）。具体的には、パケットに付されている送信元ＭＡＣアドレスを第一仮ＭＡＣアドレスに、パケットに付されている送信元ＩＰアドレスを第一仮ＩＰアドレスに、パケットに付されている送信元ポート番号を索引ポート番号に、パケットに付されている宛先ＭＡＣアドレスを内側ＮＩＣＭＡＣアドレスに、パケットに付されている宛先ＩＰアドレスを内側ＮＩＣＩＰアドレスに書き換える。そして、宛先ポート番号は変更しない。

アドレス置換部６０２はＩＰアドレス等の置換処理を行った後、当該ＴＣＰデータパケットをＴＣＰ／ＩＰプロトコルスタック２０５に送信して（Ｓ１１０６）、一連の処理を終了する（Ｓ１１０４）。

【００７６】

図１２は、アドレス変換処理部２０３の、外側ＮＩＣ１０８におけるパケット受信処理の動作の流れを示すフローチャートである。これは外側ＮＩＣ受信処理部５０２の動作の流れに該当する。

処理を開始すると（Ｓ１２０１）、受信パケット判定部７０１は、最初に外側ＮＩＣ１０８が受信したパケットが、例えばＡＲＰパケットやＩＣＭＰパケット等の、明らかに転送対象となる処理対象外パケットであるか否かを判定する（Ｓ１２０２）。

判定の結果、受信したパケットが、ＡＲＰパケットやＩＣＭＰパケット等の、明らかに転送対象となる処理対象外パケットである場合は（Ｓ１２０２のＹＥＳ）、受信パケット判定部７０１はそのパケットをそのまま内側ＮＩＣ１０４へ転送して（Ｓ１２０３）、一連の処理を終了する（Ｓ１２０４）。

【００７７】

ステップＳ１２０２において、受信したパケットが、明らかに転送対象となる処理対象外パケットでない場合（Ｓ１２０２のＮＯ）は、受信パケット判定部７０１は次にそのパケットがＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットであるか否かを判定する（Ｓ１２０５）。

判定の結果、受信したパケットが、ＸＰＴＣＰゲートウェイ装置１０１に対して送信さ

れた、ＸＰＴＣＰ処理対象外パケットである場合は（Ｓ１２０５のＹＥＳ）、受信パケット判定部７０１はそのパケットをそのままＴＣＰ／ＩＰプロトコルスタック２０５へ転送して（Ｓ１２０６）、一連の処理を終了する（Ｓ１２０４）。

【００７８】

ステップＳ１２０５において、受信したパケットが、ＸＰＴＣＰゲートウェイ装置１０１に対して送信された、ＸＰＴＣＰ処理対象外パケットでない場合は（Ｓ１２０５のＮＯ）、受信パケット判定部７０１は次に当該パケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号でＸＰＴＣＰ処理対象マスタ２０８を検索する（Ｓ１２０７）。

検索の結果、受信したパケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号の組み合わせが、ＸＰＴＣＰ処理対象マスタ２０８になければ（Ｓ１２０８のＮＯ）、当該パケットはＸＰＴＣＰゲートウェイ装置１０１の処理対象外なので、受信パケット判定部７０１はそのパケットをそのまま内側ＮＩＣ１０４へ転送して（Ｓ１２０３）、一連の処理を終了する（Ｓ１２０４）。

【００７９】

ステップＳ１２０８において、受信したパケットの送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス及び宛先ポート番号の組み合わせが、ＸＰＴＣＰ処理対象マスタ２０８にあれば（Ｓ１２０８のＹＥＳ）、当該パケットはＸＰＴＣＰゲートウェイ装置１０１の処理対象であり、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える必要がある。そこで、受信パケット判定部７０１は更に受信したパケットの詳細を見る。

受信パケット判定部７０１は、受信したパケットがＴＣＰ　ＦＩＮパケットであるか否かを判定する（Ｓ１２０９）。

判定の結果、受信したパケットがＴＣＰ　ＦＩＮパケットであれば（Ｓ１２０９のＹＥＳ）、受信パケット判定部７０１は当該ＴＣＰ　ＦＩＮパケットを索引ポート番号と共にレコード削除処理部７０３に引き渡す。

レコード削除処理部７０３は、当該ＴＣＰ　ＦＩＮパケットの索引ポート番号が削除予定リスト６０５にあることを確認したら、内側ＮＩＣアドレステーブル２０９の、当該索引ポート番号に係るレコードのタイマ用カウンタ値フィールドに、アドレステーブル更新カウンタ２１３の値を書き込む（Ｓ１２１０）。

その後、レコード削除処理部７０３はＴＣＰ　ＦＩＮパケットと索引ポート番号をアドレス置換部７０２に引き渡す。

【００８０】

アドレス置換部７０２は、受信パケット判定部７０１からレコード削除処理部７０３を通じて引き渡された索引ポート番号と仮ＩＰＭＡＣリスト２０４を参照して、ＴＣＰ　ＦＩＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き換える（Ｓ１２１１）。具体的には、

・パケットに付されている送信元ＭＡＣアドレスを第二仮ＭＡＣアドレスに、
・パケットに付されている送信元ＩＰアドレスを第二仮ＩＰアドレスに、
・パケットに付されている送信元ポート番号を索引ポート番号に、
・パケットに付されている宛先ＭＡＣアドレスを外側ＮＩＣＭＡＣアドレスに、
・パケットに付されている宛先ＩＰアドレスを外側ＮＩＣＩＰアドレスに、
・パケットに付されている宛先ポート番号を動的ポート番号に

書き換える。

アドレス置換部７０２はＩＰアドレス等の置換処理を行った後、当該ＴＣＰ　ＦＩＮパケットをＴＣＰ／ＩＰプロトコルスタック２０５に送信して（Ｓ１２０６）、一連の処理を終了する（Ｓ１２０４）。

【００８１】

ステップＳ１２０９において、受信したパケットがＴＣＰ　ＦＩＮパケットでなければ（

Ｓ１２０９のＮＯ）、当該パケットはＴＣＰデータパケットである。そこで、受信パケット判定部７０１は当該ＴＣＰデータパケットを索引ポート番号と共にアドレス置換部７０２に引き渡す。

【００８２】

アドレス置換部７０２は、受信パケット判定部７０１から引き渡された索引ポート番号と仮ＩＰＭＡＣリスト２０４を参照して、ＴＣＰデータパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書き換える（Ｓ１２１２）。具体的には、パケットに付されている送信元ＭＡＣアドレスを第二仮ＭＡＣアドレスに、パケットに付されている送信元ＩＰアドレスを第二仮ＩＰアドレスに、パケットに付されている送信元ポート番号を索引ポート番号に、パケットに付されている宛先ＭＡＣアドレスを外側ＮＩＣＭＡＣアドレスに、パケットに付されている宛先ＩＰアドレスを外側ＮＩＣＩＰアドレスに、パケットに付されている宛先ポート番号を動的ポート番号に書き換える。

アドレス置換部７０２はＩＰアドレス等の置換処理を行った後、当該ＴＣＰデータパケットをＴＣＰ／ＩＰプロトコルスタック２０５に送信して（Ｓ１２０６）、一連の処理を終了する（Ｓ１２０４）。

【００８３】

図１３は、アドレス変換処理部２０３の、外側ＮＩＣ１０８におけるパケット送信処理の動作の流れを示すフローチャートである。これは外側ＮＩＣ送信処理部５０３の動作の流れに該当する。

処理を開始すると（Ｓ１３０１）、送信パケット判定部は、最初にＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットの種別と宛先ＩＰアドレスを見る。

パケットの種別がＩＣＭＰパケットやＵＤＰパケットである場合、パケットの種別がＡＲＰ要求パケットで且つ探索ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第二仮ＩＰアドレスでない場合、パケットの種別がＴＣＰパケットであって且つ宛先ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第二仮ＩＰアドレスではない場合は（Ｓ１３０２のＮＯ）、これらのパケットはＸＰＴＣＰゲートウェイ装置１０１が処理していないパケットである。そこで、送信パケット判定部はそのパケットに対して何ら加工せず、そのまま外側ＮＩＣ１０８を通じて送信して（Ｓ１３０３）、一連の処理を終了する（Ｓ１３０４）。

【００８４】

ステップＳ１３０２において、ＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットの種別がＴＣＰパケットであって且つ宛先ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第二仮ＩＰアドレスである場合、又はＡＲＰ要求パケットであって且つ探索ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第二仮ＩＰアドレスである場合（Ｓ１３０２のＹＥＳ）は、更に当該パケットがＡＲＰ要求パケットであるか否かを判定する（Ｓ１３０５）。

ＡＲＰ要求パケットであって且つ探索ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第二仮ＩＰアドレスである場合（Ｓ１３０５のＹＥＳ）は、このＡＲＰ要求パケットはＴＣＰ／ＩＰプロトコルスタック２０５が実在しない第二仮ＩＰアドレスに対してパケットを送信しようとした結果、生成されたパケットである。このＡＲＰ要求パケットは外側ＮＩＣ１０８から送信させるのではなく、第二仮ＩＰアドレスと同様に実在しないＭＡＣアドレスである第二仮ＭＡＣアドレスで、ＡＲＰ応答パケットを生成して返答しなければならない。そこで、送信パケット判定部は当該ＡＲＰ要求パケットをＡＲＰ応答処理部８０２に引き渡す。

ＡＲＰ応答処理部８０２は、送信パケット判定部からＡＲＰ要求パケットを受け取ると、仮ＩＰＭＡＣリストを参照して、第二仮ＭＡＣアドレスでＡＲＰ応答パケットを生成して、ＴＣＰ／ＩＰプロトコルスタック２０５に返送して（Ｓ１３０６）、一連の処理を終了する（Ｓ１３０４）。

【００８５】

ステップＳ１３０５において、ＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットがＴＣＰパケットであって且つ宛先ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第二仮ＩＰアドレスである場合は（Ｓ１３０５のＮＯ）、当該パケットはＸＰＴＣＰゲートウェイ装置１０１が処理したパケットであり、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を、内側ＮＩＣ受信処理部５０１が書き換える以前の状態に書き戻す必要がある。そこで、送信パケット判定部は更に受信したパケットの詳細を見る。

【００８６】

送信パケット判定部は、ＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットがＴＣＰ　ＳＹＮパケットであるか否かを判定する（Ｓ１３０７）。

判定の結果、ＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットがＴＣＰ　ＳＹＮパケットであれば（Ｓ１３０７のＹＥＳ）、当該ＴＣＰ　ＳＹＮパケットはコネクションが新たに生成されたことを示すパケットである。その際、ＴＣＰ／ＩＰプロトコルスタック２０５がコネクションを生成する際に、送信元ポート番号として動的ポート番号を自動的に付与している。この動的ポート番号を、外側ＮＩＣアドレステーブル２１０に記憶しておく必要がある。そこで、送信パケット判定部は当該ＴＣＰ　ＳＹＮパケットを動的ポート記録処理部８０３に引き渡す。

動的ポート記録処理部８０３は、ＴＣＰ　ＳＹＮパケットを受け取ると、先ずＴＣＰ　ＳＹＮパケットの送信元ポート番号を取得する。次に、宛先ポート番号に記されている索引ポート番号で外側ＮＩＣアドレステーブル２１０を検索し、特定したレコードの動的ポート番号フィールドに、先に取得したＴＣＰ　ＳＹＮパケットの送信元ポート番号を書き込む（Ｓ１３０８）。

こうして、コネクションの開始を示すＴＣＰ　ＳＹＮパケットに付されている動的ポート番号を記憶しておくことで、これ以降に当該コネクションを経由するパケットのＩＰアドレス等を正しく置換又は復元することができる。

【００８７】

動的ポート記録処理部８０３は、動的ポート番号の記録を行った後、ＴＣＰ　ＳＹＮパケットをアドレス復元部９０２に引き渡す。

アドレス復元部９０２は、先に動的ポート記録処理部８０３が特定した外側ＮＩＣアドレステーブル２１０のレコードを参照して、ＴＣＰ　ＳＹＮパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を復元する（Ｓ１３０９）。そして、当該ＴＣＰ ＳＹＮパケットを外側ＮＩＣ１０８を通じて送信して（Ｓ１３０３）、一連の処理を終了する（Ｓ１３０４）。

【００８８】

ステップＳ１３０７において、ＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットがＴＣＰ　ＳＹＮパケットでなければ（Ｓ１３０７のＮＯ）、送信パケット判定部は当該ＴＣＰパケットをアドレス復元部９０２に引き渡す。

アドレス復元部９０２は、ＴＣＰパケットの宛先ポート番号に付されている索引ポート番号で外側ＮＩＣアドレステーブル２１０のレコードを検索してレコードを特定し、ＴＣＰパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を復元する（Ｓ１３０９）。そして、当該ＴＣＰ ＳＹＮパケットを外側ＮＩＣ１０８を通じて送信して（Ｓ１３０３）、一連の処理を終了する（Ｓ１３０４）。

【００８９】

図１４は、アドレス変換処理部２０３の、内側ＮＩＣ１０４におけるパケット送信処理の動作の流れを示すフローチャートである。これは内側ＮＩＣ送信処理部５０４の動作の流れに該当する。

処理を開始すると（Ｓ１４０１）、送信パケット判定部は、最初にＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットの種別と宛先ＩＰアドレスを見る。

パケットの種別がＩＣＭＰパケットやＡＲＰパケットやＵＤＰパケットである場合、パケットの種別がＴＣＰパケットであって且つ宛先ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第一仮ＩＰアドレスではない場合は（Ｓ１４０２のＮＯ）、これらのパケットはＸＰＴＣＰゲートウェイ装置１０１が処理していないパケットである。そこで、送信パケット判定部はそのパケットに対して何ら加工せず、そのまま内側ＮＩＣ１０４を通じて送信して（Ｓ１４０３）、一連の処理を終了する（Ｓ１４０４）。

【００９０】

ステップＳ１４０２において、ＴＣＰ／ＩＰプロトコルスタック２０５から受け取ったパケットの種別がＴＣＰパケットであって且つ宛先ＩＰアドレスが仮ＩＰＭＡＣリスト２０４に記されている第一仮ＩＰアドレスである場合（Ｓ１４０２のＹＥＳ）は、当該パケットはＸＰＴＣＰゲートウェイ装置１０１が処理したパケットであり、パケットに付されているＭＡＣアドレス、ＩＰアドレス及びポート番号を、内側ＮＩＣ受信処理部５０１が書き換える以前の状態に書き戻す必要がある。そこで、送信パケット判定部は当該ＴＣＰパケットをアドレス復元部９０２に引き渡す。

アドレス復元部９０２は、ＴＣＰパケットの宛先ポート番号に付されている索引ポート番号で内側ＮＩＣアドレステーブル２０９のレコードを検索してレコードを特定し、ＴＣＰパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を復元する（Ｓ１４０５）。そして、当該ＴＣＰ ＳＹＮパケットを内側ＮＩＣ１０４を通じて送信して（Ｓ１４０３）、一連の処理を終了する（Ｓ１４０４）。

【００９１】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・ＸＰＴＣＰ処理部２０６の動作］

図１５は、ＸＰＴＣＰ処理部２０６のＸＰＴＣＰ処理の流れを示すフローチャートである。

ＸＰＴＣＰ処理とは、ＴＣＰ又はＵＤＰパケットに対し、トランスポート層において所定の認証及び暗号化処理を施す処理である。ＸＰＴＣＰ処理の基本的な技術内容は特許文献１に開示されているので、本実施形態では詳細には説明しない。その代わり、前述のアドレス変換処理部２０３及び後述するソケット処理部２０７で行っている、ソケットの処理に関係する内容を説明する。

【００９２】

処理を開始すると（Ｓ１５０１）、イベント検出部１００１はソケット処理部２０７から内側ＮＩＣ１０４に対するコネクションに係るａｃｃｅｐｔイベントを検出したか否かを確認する（Ｓ１５０２）。ａｃｃｅｐｔイベントを検出したなら（Ｓ１５０２のＹＥＳ）、イベント検出部１００１はソケット操作部１００２を制御して、当該ａｃｃｅｐｔイベントに係る、生成されたソケットの、ソケットメモリ領域１００４内におけるアドレスを取得する（Ｓ１５０３）。そして、イベント検出部１００１はポリシー設定部１００３を起動する。

ポリシー設定部１００３は当該ａｃｃｅｐｔイベントに係るソケットに関し、索引ポート番号にてアドレス変換処理部２０３に対してポリシーの問い合わせを行う。アドレス変換処理部２０３のポリシー回答部５０６は、内側ＮＩＣアドレステーブル２０９を索引ポート番号で検索してレコードを特定する。そして、特定したレコードの送信元ＩＰアドレス及びポート番号、宛先ＩＰアドレス及びポート番号を用いてＸＰＴＣＰ処理対象マスタ２０８を検索し、レコードを特定し、当該レコードのレコード番号を取得したら、そのレコード番号をポリシー設定部１００３へ回答する。ポリシー設定部１００３は、得られたレコード番号と索引ポート番号を、ＸＰＴＣＰポリシーテーブル２１１に記録して、紐付ける。この時点で、暗号化処理部１００５は索引ポート番号を手がかりに、ＸＰＴＣＰ処理対象マスタ２０８のレコードを特定して、暗号化のポリシーを設定することができる（Ｓ１５０４）。そして、一連の処理を終了する（Ｓ１５０５）。

【００９３】

ステップＳ１５０２において、ａｃｃｅｐｔイベントを検出できなかったなら（Ｓ１５

０２のＮＯ）、イベント検出部１００１は次にＴＣＰ／ＩＰプロトコルスタック２０５から外側ＮＩＣ１０８に対するコネクションに係るｃｏｎｎｅｃｔ応答イベントを検出したか否かを確認する（Ｓ１５０６）。ｃｏｎｎｅｃｔ応答イベントを検出したなら（Ｓ１５０６のＹＥＳ）、イベント検出部１００１はソケット操作部１００２を制御して、当該ｃｏｎｎｅｃｔ応答イベントに係る、生成されたソケットの、ソケットメモリ領域１００４内におけるアドレスを取得する（Ｓ１５０７）。

【００９４】

次に、イベント検出部１００１は索引ポート番号を共有する、内側ＮＩＣ１０４に対するコネクションに係るソケットと、外側ＮＩＣ１０８に対するコネクションに係るソケットとの関連付けを行う（Ｓ１５０８）。この時点で、復号処理部１００６は索引ポート番号を手がかりに、ＸＰＴＣＰ処理対象マスタ２０８のレコードを特定して、復号のポリシーを設定することができる（Ｓ１５０９）。そして、一連の処理を終了する（Ｓ１５０５）。

【００９５】

こうすることで、内側ＮＩＣ１０４に対するコネクションに係るソケットから得られたストリームデータは、暗号化処理部１００５を通じて暗号化され、暗号化されたストリームデータは外側ＮＩＣ１０８に対するコネクションに係るソケットに出力される。また逆に、外側ＮＩＣ１０８に対するコネクションに係るソケットから得られたストリームデータは、復号処理部１００６を通じて復号され、復号されたストリームデータは内側ＮＩＣ１０４に対するコネクションに係るソケットに出力される。

【００９６】

ステップＳ１５０６において、ｃｏｎｎｅｃｔ応答イベントを検出できなかったなら（Ｓ１５０６のＮＯ）、イベント検出部１００１は次にＴＣＰ／ＩＰプロトコルスタック２０５から外側ＮＩＣ１０８に対するコネクションに係るｃｌｏｓｅイベントを検出したか否かを確認する（Ｓ１５１０）。ｃｌｏｓｅイベントを検出したなら（Ｓ１５１０のＹＥＳ）、イベント検出部１００１はソケット操作部１００２を制御して、当該ｃｌｏｓｅイベントに係る、生成されたソケット同士の関連付けを開放すると共に、ＸＰＴＣＰポリシーテーブル２１１の該当レコードを削除する（Ｓ１５１１）。そして、一連の処理を終了する（Ｓ１５０５）。

【００９７】

ステップＳ１５１０において、ｃｌｏｓｅイベントを検出できなかったなら（Ｓ１５１０のＮＯ）、イベント検出部１００１は特に何もしない。その代わり、暗号化処理部１００５及び復号処理部１００６は、ソケット操作部１００２からストリームデータを受け取り、ＸＰＴＣＰポリシーテーブル２１１で特定した暗号化又は復号ポリシーに基づいて暗号化又は復号処理を実行し（Ｓ１５１２）、ソケット操作部１００２はそれら処理されたストリームデータを転送する（Ｓ１５１３）。そして、一連の処理を終了する（Ｓ１５０５）。

【００９８】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・ソケット処理部２０７の動作］

図１６は、ソケット処理部２０７の初期動作の流れを示すフローチャートである。

処理を開始すると（Ｓ１６０１）、ソケット処理部２０７は予め定められたポート番号に対する、ＴＣＰサーバ機能を起動する（Ｓ１６０２）。この時、内側ＮＩＣ１０４に向けてリクエストを受け付けるためのソケットが作成され（ｓｏｃｋｅｔ関数）、当該ソケットにはリクエストを受け付ける際のポート番号が定義される（ｂｉｎｄ関数）。そして、一連の処理を終了する（Ｓ１６０３）。

【００９９】

図１７は、ソケット処理部２０７の接続要求転送処理の流れを示すフローチャートである。

ソケット処理部２０７は、ＴＣＰ／ＩＰプロトコルスタック２０５からｃｏｎｎｅｃｔイベントを受け取ると（Ｓ１３０１）、ソケットを通じて内側ＮＩＣ１０４に対して接続

許可を示すａｃｃｅｐｔイベントを発行する（Ｓ１７０２）。これはサーバとしての振る舞いである。次にソケット処理部２０７は、外側ＮＩＣ１０８に向けて、接続を要求するｃｏｎｎｅｃｔ　ｒｅｑｕｅｓｔイベントを発行する（Ｓ１７０３）。これはクライアントとしての振る舞いである。そして、一連の処理を終了する（Ｓ１７０４）。

【０１００】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・アドレス変換処理部２０３によるパケットの変化］

図１８、図１９及び図２０は、ＸＰＴＣＰゲートウェイ装置１０１を通過するパケットの変化を示す概略図である。

ＸＰＴＣＰ非対応ＰＣ１０３には、第一ＭＡＣアドレスと第一ＩＰアドレスが付与されている。

ＸＰＴＣＰ対応サーバ１０７には、第二ＭＡＣアドレスと第二ＩＰアドレスが付与されている。

ＸＰＴＣＰ非対応ＰＣ１０３からＸＰＴＣＰ対応サーバ１０７に向けてパケットが送信されると、送信パケットは内側ＮＩＣ１０４を通じて、アドレス変換処理部２０３に到達する。アドレス変換処理部２０３は内側ＮＩＣアドレステーブル２０９を参照して、アドレス変換処理を施す。すると、送信パケットはアドレス変換処理済み送信パケットに変化する。

アドレス変換処理済み送信パケットは、宛先ＩＰアドレスが内側ＮＩＣ１０４のＩＰアドレスである。したがって、ＴＣＰ／ＩＰプロトコルスタック２０５はアドレス変換処理済み送信パケットを受け入れ、パケットからＭＡＣヘッダ、ＩＰヘッダ、ＴＣＰヘッダの順にヘッダを除去し、ペイロードを連結してストリームデータを復元する。復元されたストリームデータはソケットを通じてＸＰＴＣＰ処理部に到達する。ＸＰＴＣＰ処理部はストリームデータに所定の暗号化処理を施す。そして、暗号化されたストリームデータは外側ＮＩＣ１０８に向けて作成されたソケットに供給される。

【０１０１】

ＴＣＰ／ＩＰプロトコルスタック２０５は暗号化されたストリームデータを所定のバイト長に区切って、ＴＣＰヘッダ、ＩＰヘッダ及びＭＡＣヘッダを付加し、暗号化及びアドレス変換処理済み送信パケットを作成する。つまり、この時点で作成されたパケットの宛先ＩＰアドレスは、第二仮ＩＰアドレスであり、本来の送信先であるＸＰＴＣＰ対応サーバ１０７のＩＰアドレス（第二ＩＰアドレス）ではない。そこで、アドレス変換処理部は外側ＮＩＣアドレステーブル２１０を参照して、アドレス復元処理を施す。すると、暗号化及びアドレス変換処理済み送信パケットは、暗号化処理済み送信パケットとなって、ＸＰＴＣＰ対応サーバ１０７に到達する。

【０１０２】

ＸＰＴＣＰ対応サーバ１０７からＸＰＴＣＰ非対応ＰＣ１０３に向けて暗号化処理済み受信パケットが返送されると、暗号化処理済み受信パケットは外側ＮＩＣ１０８を通じて、アドレス変換処理部２０３に到達する。アドレス変換処理部２０３は外側ＮＩＣアドレステーブル２１０を参照して、アドレス変換処理を施す。すると、暗号化処理済み受信パケットは暗号化及びアドレス変換処理済み受信パケットに変化する。

暗号化及びアドレス変換処理済み受信パケットは、宛先ＩＰアドレスが外側ＮＩＣ１０８のＩＰアドレスである。したがって、ＴＣＰ／ＩＰプロトコルスタック２０５は暗号化及びアドレス変換処理済み受信パケットを受け入れ、パケットからＭＡＣヘッダ、ＩＰヘッダ、ＴＣＰヘッダの順にヘッダを除去し、ペイロードを連結して暗号化ストリームデータを復元する。復元された暗号化ストリームデータはソケットを通じてＸＰＴＣＰ処理部に到達する。ＸＰＴＣＰ処理部はストリームデータに所定の復号処理を施す。そして、復号されたストリームデータは外側ＮＩＣ１０８に向けて作成されたソケットに供給される。

【０１０３】

ＴＣＰ／ＩＰプロトコルスタック２０５は復号されたストリームデータを所定のバイト

長に区切って、ＴＣＰヘッダ、ＩＰヘッダ及びＭＡＣヘッダを付加し、アドレス変換処理済み受信パケットを作成する。つまり、この時点で作成されたパケットの宛先ＩＰアドレスは、第一仮ＩＰアドレスであり、本来の送信先であるＸＰＴＣＰ非対応ＰＣ１０３のＩＰアドレス（第一ＩＰアドレス）ではない。そこで、アドレス変換処理部は内側ＮＩＣアドレステーブル２０９を参照して、アドレス復元処理を施す。すると、アドレス変換処理済み受信パケットは、受信パケットとなって、ＸＰＴＣＰ非対応ＰＣ１０３に到達する。

【０１０４】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・ＴＣＰ接続確立シーケンス］

図２１、図２２及び図２３は、ＸＰＴＣＰゲートウェイ装置１０１における、ＴＣＰ接続確立シーケンスのタイムチャートである。図２１はタイムチャート全体を示す俯瞰図であり、図２２はタイムチャートのうち、前半の処理内容を示す詳細図であり、図２３はタイムチャートのうち、後半の処理内容を示す詳細図である。

端末からＴＣＰ ＳＹＮパケットが送信されたことに呼応して、端末とＸＰＴＣＰゲートウェイ装置１０１との間と、サーバとＸＰＴＣＰゲートウェイ装置１０１都の間との夫々に、ＴＣＰコネクションが形成される迄の、ＸＰＴＣＰゲートウェイ装置１０１の時系列上の動作の推移を示す。

【０１０５】

ＸＰＴＣＰ非対応ＰＣ１０３がｗｅｂブラウザ等のアプリケーションプログラムを動作させて、ＸＰＴＣＰ対応サーバ１０７へ接続しようとすると、ＸＰＴＣＰ非対応ＰＣ１０３はアプリケーションプログラムに起因してＴＣＰ ＳＹＮパケットを送信する（Ｓ２１０１）。

ＴＣＰ ＳＹＮパケットは、内側ＮＩＣ１０４を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ受信処理部５０１は、ＴＣＰ ＳＹＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２１０２）。なお、この時点で内側ＮＩＣアドレステーブル２０９に新規レコードが追記録され、当該レコードは索引ポート番号で特定可能になる。

【０１０６】

アドレス変換処理を施されたＴＣＰ ＳＹＮパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ソケット処理部２０７が予め作成していたポート番号に対して送信されたＴＣＰ ＳＹＮパケットを認識して、コネクションの作成を開始するために、ソケット処理部２０７に対してｃｏｎｎｅｃｔイベントを発行する（Ｓ２１０３）。

ソケット処理部２０７は、自身のサーバ機能によって、ｃｏｎｎｅｃｔイベント（接続要求）に対するａｃｃｅｐｔイベント（接続許可）を、ＴＣＰ／ＩＰプロトコルスタック２０５に対して発行する（Ｓ２１０４）。

【０１０７】

ＸＰＴＣＰ処理部２０６は、このａｃｃｅｐｔイベントをフックして、内側ＮＩＣ１０４に向けたコネクションの形成が始まったことを認識する（Ｓ２１０５）。すると、ＸＰＴＣＰ処理部２０６はアドレス変換処理部２０３に対して、索引ポート番号を伴って当該コネクションに適用するポリシーを問い合わせる（Ｓ２１０６）。アドレス変換処理部２０３はこの問い合わせに対してＸＰＴＣＰ処理対象マスタ２０８と内側ＮＩＣアドレステーブル２０９を参照して、ＸＰＴＣＰ処理対象マスタ２０８のレコード番号を回答する（Ｓ２１０７）。ＸＰＴＣＰ処理部２０６はＸＰＴＣＰポリシーテーブル２１１にレコード番号と索引ポート番号を登録して紐付けて、復号処理部１００６のポリシーを設定する（Ｓ２１０８）。

【０１０８】

ステップＳ２１０４にて発行されたａｃｃｅｐｔイベントはＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５はａｃｃｅｐｔイベントを受けて、ＴＣＰ ＡＣＫ／ＳＹＮパケットを生成する（Ｓ２１０９）。ＴＣＰ ＡＣＫ／ＳＹＮパケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３

の内側ＮＩＣ送信処理部５０４は、ＴＣＰ ＡＣＫ／ＳＹＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を復元する（Ｓ２１１０）。

ＴＣＰ ＡＣＫ／ＳＹＮパケットは、内側ＮＩＣ１０４を通じてＸＰＴＣＰ非対応ＰＣ１０３に到達する。ＸＰＴＣＰ非対応ＰＣ１０３は、ＴＣＰ ＡＣＫ／ＳＹＮパケットを受けて、ＴＣＰ ＡＣＫパケットで応答する（Ｓ２１１１）。

【０１０９】

ＴＣＰ ＡＣＫパケットは、内側ＮＩＣ１０４を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ受信処理部５０１は、ＴＣＰ ＡＣＫパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２１１２）。

【０１１０】

アドレス変換処理を施されたＴＣＰ ＡＣＫパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ＴＣＰ ＡＣＫパケットの到着を以て、コネクションが確立したことを認識する（Ｓ２１１３）。これ以降、当該コネクションにはＴＣＰデータパケットが送受信される。

【０１１１】

ソケット処理部２０７は、ステップＳ２１０４にて内側ＮＩＣ１０４に向けてサーバ機能としてのａｃｃｅｐｔイベントを発行した後、外側ＮＩＣ１０８に向けてクライアント機能として接続要求を示すｃｏｎｎｅｃｔ ｒｅｑｕｅｓｔイベントを発行する（Ｓ２１１４）。

ｃｏｎｎｅｃｔ ｒｅｑｕｅｓｔイベントはＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５はｃｏｎｎｅｃｔ ｒｅｑｕｅｓｔイベントを受けて、ＡＲＰ要求パケットを生成する（Ｓ２１１５）。

ＡＲＰ要求パケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ送信処理部５０３は、ＡＲＰ要求パケットに対するＡＲＰ応答パケットを生成し、ＴＣＰ／ＩＰプロトコルスタック２０５に返送する（Ｓ２１１６）。

ＴＣＰ／ＩＰプロトコルスタック２０５は、ＡＲＰ応答パケットを受け取ると、ステップＳ２１１４におけるｃｏｎｎｅｃｔ ｒｅｑｕｅｓｔイベントに対応するＴＣＰ ＳＹＮパケットを生成する準備が整ったので、ＴＣＰ ＳＹＮパケットを生成する（Ｓ２１１７）。

ステップＳ２１１７にて生成されるＴＣＰ ＳＹＮパケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ送信処理部５０３は、ＴＣＰ ＳＹＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２１１８）。なお、この時点で外側ＮＩＣアドレステーブル２１０の該当レコードに、ＴＣＰ ＳＹＮパケットの送信元ポート番号として、ＴＣＰ／ＩＰプロトコルスタック２０５によって自動的に付されている動的ポート番号が記録される。

【０１１２】

ＴＣＰ ＳＹＮパケットは、外側ＮＩＣ１０８を通じてＸＰＴＣＰ対応サーバ１０７に到達する。ＸＰＴＣＰ対応サーバ１０７は、ＴＣＰ ＳＹＮパケットを受けて、ＴＣＰ ＡＣＫ／ＳＹＮパケットで応答する（Ｓ２１１９）。

ＴＣＰ ＡＣＫ／ＳＹＮパケットは、外側ＮＩＣ１０８を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ受信処理部５０２は、ＴＣＰ ＡＣＫ／ＳＹＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２１２０）。

アドレス変換処理を施されたＴＣＰ ＡＣＫ／ＳＹＮパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ＴＣＰ ＡＣＫ／ＳＹＮパケットを受けて、ＴＣＰ ＡＣＫパケットで応答する（Ｓ２１２１）。このとき、ＴＣＰ／ＩＰプロトコルスタック２０５はｃｏｎｎｅｃｔ応答イベントをクライアントプログラムであるソケット処理部２０７に通知する。

【０１１３】

ＸＰＴＣＰ処理部２０６は、このｃｏｎｎｅｃｔ応答イベントをフックして、外側ＮＩＣ１０８に向けたコネクションの形成が始まったことを認識する（Ｓ２１２２）。すると、ＸＰＴＣＰ処理部２０６はアドレス変換処理部２０３に対して、索引ポート番号を伴って当該コネクションに適用するポリシーを問い合わせる（Ｓ２１２３）。アドレス変換処理部２０３はこの問い合わせに対してＸＰＴＣＰ処理対象マスタ２０８と内側ＮＩＣアドレステーブル２０９を参照して、ＸＰＴＣＰ処理対象マスタ２０８のレコード番号を回答する（Ｓ２１２４）。ＸＰＴＣＰ処理部２０６はＸＰＴＣＰポリシーテーブル２１１にレコード番号と索引ポート番号を登録して紐付けて、暗号化処理部１００５のポリシーを設定する（Ｓ２１２５）。

【０１１４】

ステップＳ２１２１にてＴＣＰ／ＩＰプロトコルスタック２０５から発行されたＴＣＰ ＡＣＫパケットは、アドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ送信処理部５０３は、ＴＣＰ ＡＣＫパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を復元する（Ｓ２１２６）。

ＴＣＰ ＡＣＫパケットは、外側ＮＩＣ１０８を通じてＸＰＴＣＰ対応サーバ１０７に到達する。ＸＰＴＣＰ対応サーバ１０７は、ＴＣＰ ＡＣＫパケットの到着を以て、コネクションが確立したことを認識する（Ｓ２１２７）。これ以降、当該コネクションにはＴＣＰデータパケットが送受信される。

【０１１５】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・ＴＣＰデータ転送シーケンス］

図２４は、ＸＰＴＣＰゲートウェイ装置１０１における、ＴＣＰデータ転送シーケンスのタイムチャートである。端末からＴＣＰデータパケットが送信されたことに呼応して、端末とＸＰＴＣＰゲートウェイ装置１０１との間と、サーバとＸＰＴＣＰゲートウェイ装置１０１都の間との夫々に形成されたＴＣＰコネクションにＴＣＰデータパケットが通過する際の、ＸＰＴＣＰゲートウェイ装置１０１の時系列上の動作の推移を示す。

【０１１６】

ＸＰＴＣＰ非対応ＰＣ１０３がｗｅｂブラウザ等のアプリケーションプログラムを動作させて、ＸＰＴＣＰ対応サーバ１０７へデータを送信しようとすると、ＸＰＴＣＰ非対応ＰＣ１０３はアプリケーションプログラムに起因してＴＣＰデータパケットを送信する（Ｓ２４０１）。

ＴＣＰデータパケットは、内側ＮＩＣ１０４を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ受信処理部５０１は、ＴＣＰデータパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２４０２）。

【０１１７】

アドレス変換処理を施されたＴＣＰデータパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ＴＣＰデータパケットのヘッダを除去して、ＴＣＰデータパケットペイロードを連結し、ストリームデータに復元する（Ｓ２４０３）。

ストリームデータはＸＰＴＣＰ処理部２０６によって暗号化処理が施され、外側ＮＩＣ１０８のソケットに転送される（Ｓ２４０４）。

【０１１８】

暗号化処理を施されたストリームデータは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ストリームデータを所定のバイト長毎に分割した後、ヘッダを付加して、ＴＣＰデータパケットに変換する（Ｓ２４０５）。

【０１１９】

ＴＣＰデータパケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ送信処理部５０３は、ＴＣＰデータパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２４０６）。

アドレス復元処理を施されたＴＣＰデータパケットは、外側ＮＩＣ１０８を通じてＸＰＴＣＰ対応サーバ１０７に到達する（Ｓ２４０７）。ＸＰＴＣＰ対応サーバ１０７は、ＴＣＰデータパケットを受けて、所定の処理を行った後、返信データとしてのＴＣＰデータパケットを、ＸＰＴＣＰ非対応ＰＣ１０３に向けて送信する（Ｓ２４０８）。

【０１２０】

ＴＣＰデータパケットは、外側ＮＩＣ１０８を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ受信処理部５０２は、ＴＣＰデータパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２４０９）。

アドレス変換処理を施されたＴＣＰデータパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ＴＣＰデータパケットのヘッダを除去して、ＴＣＰデータパケットペイロードを連結し、ストリームデータに復元する（Ｓ２４１０）。

ストリームデータはＸＰＴＣＰ処理部２０６によって復号処理が施され、内側ＮＩＣ１０４のソケットに転送される（Ｓ２４１１）。

【０１２１】

復号処理を施されたストリームデータは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ストリームデータを所定のバイト長毎に分割した後、ヘッダを付加して、ＴＣＰデータパケットに変換する（Ｓ２４１２）。

ＴＣＰデータパケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ送信処理部５０４は、ＴＣＰデータパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２４１３）。

アドレス復元処理を施されたＴＣＰデータパケットは、内側ＮＩＣ１０４を通じてＸＰＴＣＰ非対応ＰＣ１０３に到達する（Ｓ２４１４）。

【０１２２】

［ＸＰＴＣＰゲートウェイ装置１０１の動作・ＴＣＰ切断シーケンス］

図２５、図２６及び図２７は、ＸＰＴＣＰゲートウェイ装置１０１における、ＴＣＰ切断シーケンスのタイムチャートである。図２５はタイムチャート全体を示す俯瞰図であり、図２６はタイムチャートのうち、前半の処理内容を示す詳細図であり、図２７はタイムチャートのうち、後半の処理内容を示す詳細図である。

端末からＴＣＰ ＦＩＮパケットが送信されたことに呼応して、端末とＸＰＴＣＰゲートウェイ装置１０１との間と、サーバとＸＰＴＣＰゲートウェイ装置１０１との間の夫々に形成されていたＴＣＰコネクションを終了（ｃｌｏｓｅ：クローズ）される迄の、ＸＰＴＣＰゲートウェイ装置１０１の時系列上の動作の推移を示す。

【０１２３】

ＸＰＴＣＰ非対応ＰＣ１０３がｗｅｂブラウザ等のアプリケーションプログラムを動作させて、ＸＰＴＣＰ対応サーバ１０７に対して所定のデータを要求し、その要求したデータが得られたなら、ＸＰＴＣＰ非対応ＰＣ１０３はアプリケーションプログラムに起因してＴＣＰ ＦＩＮパケットを送信する（Ｓ２５０１）。

ＴＣＰ ＦＩＮパケットは、内側ＮＩＣ１０４を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ受信処理部５０１は、ＴＣＰ ＦＩＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２１０２）。なお、この時点で削除予定リスト６０５に索引ポート番号が追記録される。

【０１２４】

アドレス変換処理を施されたＴＣＰ ＦＩＮパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ソケット処理部２０７が予め作成していたポート番号に対して送信されたＴＣＰ ＦＩＮパケットを認識して、サーバプログラムであるソケット処理部２０７にコネクションの終了を通知するために、ソケット処理部２０７に対してｃｌｏｓｅイベントを発行する（Ｓ２５０３）。

【０１２５】

ソケット処理部２０７は、ステップＳ２５０３にて内側ＮＩＣ１０４に向けてサーバ機能としてのｃｌｏｓｅイベントを受け取った後、外側ＮＩＣ１０８に向けてクライアント機能として切断要求を示すｃｌｏｓｅ　ｒｅｑｕｅｓｔイベントを発行する（Ｓ２５０４）。

ｃｌｏｓｅ　ｒｅｑｕｅｓｔイベントはＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５はｃｌｏｓｅ　ｒｅｑｕｅｓｔイベントを受けて、ＴＣＰ　ＦＩＮパケットを生成する（Ｓ２５０５）。

ステップＳ２５０５にて生成されるＴＣＰ　ＦＩＮパケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ送信処理部５０３は、ＴＣＰ　ＦＩＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２５０６）。

【０１２６】

ＴＣＰ　ＦＩＮパケットは、外側ＮＩＣ１０８を通じてＸＰＴＣＰ対応サーバ１０７に到達する（Ｓ２５０７）。ＸＰＴＣＰ対応サーバ１０７は、ＴＣＰ　ＦＩＮパケットを受けて、ＸＰＴＣＰ非対応ＰＣ１０３に対して送信すべきデータを全て送信したと判断したら、ＴＣＰ　ＡＣＫ／ＦＩＮパケットを送信する（Ｓ２５０８）。

ＴＣＰ　ＡＣＫ／ＦＩＮパケットは、外側ＮＩＣ１０８を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ受信処理部５０２は、ＴＣＰ　ＡＣＫ／ＦＩＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２５０９）。

【０１２７】

アドレス変換処理を施されたＴＣＰ　ＡＣＫ／ＦＩＮパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ＴＣＰ　ＡＣＫ／ＦＩＮパケットを受けて、ＴＣＰ　ＡＣＫパケットで応答する（Ｓ２５１０）。このとき、ＴＣＰ／ＩＰプロトコルスタック２０５はｃｌｏｓｅ応答イベントをクライアントプログラムであるソケット処理部２０７に通知する。

【０１２８】

ＸＰＴＣＰ処理部２０６は、このｃｌｏｓｅ応答イベントをフックして、外側ＮＩＣ１０８に向けたコネクションと内側ＮＩＣ１０４に向けたコネクションとの関連付けを解放する（Ｓ２５１１）。

【０１２９】

ステップＳ２５１０にてＴＣＰ／ＩＰプロトコルスタック２０５によって生成されるＴＣＰ　ＡＣＫパケットは、アドレス変換処理部２０３に到達する。アドレス変換処理部２０３の外側ＮＩＣ送信処理部５０３は、ＴＣＰ　ＡＣＫパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２５１２）。

ＴＣＰ　ＡＣＫパケットは、外側ＮＩＣ１０８を通じてＸＰＴＣＰ対応サーバ１０７に到達する。ＸＰＴＣＰ対応サーバ１０７は、ＴＣＰ　ＡＣＫパケットを受けて、当該パケットに係るコネクションの切断が完了した（クローズされた）ことを認識する（Ｓ２５１３）。

【０１３０】

一方、ステップＳ２５１０にてＴＣＰ／ＩＰプロトコルスタック２０５によって生成されるｃｌｏｓｅ応答イベントは、ソケット処理部２０７に到達する。ソケット処理部２０７は、ｃｌｏｓｅ応答イベントを検出すると、外側ＮＩＣ１０８に向けたコネクションに対するＴＣＰ　ＦＩＮパケットが来たことを認識する。この時点で、対応する内側ＮＩＣ１０４に向けたコネクションの切断処理も遂行できることとなる。そこで、ステップＳ２５０３にてＴＣＰ／ＩＰプロトコルスタック２０５が送出したｃｌｏｓｅイベントに対する応答として、許可を意味するａｃｃｅｐｔイベントを、ＴＣＰ／ＩＰプロトコルスタック２０５に送出する（Ｓ２５１４）。

【０１３１】

ステップＳ２５１４にてソケット処理部２０７が送出したａｃｃｅｐｔイベントは、Ｔ

ＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５はａｃｃｅｐｔイベントを受けて、ＴＣＰ　ＡＣＫ／ＦＩＮパケットを生成する（Ｓ２５１５）。ＴＣＰ　ＡＣＫ／ＦＩＮパケットはアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ送信処理部５０４は、ＴＣＰ ＡＣＫ／ＦＩＮパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を復元する（Ｓ２５１６）。

ＴＣＰ ＡＣＫ／ＦＩＮパケットは、内側ＮＩＣ１０４を通じてＸＰＴＣＰ非対応ＰＣ１０３に到達する。ＸＰＴＣＰ非対応ＰＣ１０３は、ＴＣＰ ＡＣＫ／ＦＩＮパケットを受けて、ＴＣＰ　ＡＣＫパケットで応答する（Ｓ２５１７）。

【０１３２】

ＴＣＰ ＡＣＫパケットは、内側ＮＩＣ１０４を通じてアドレス変換処理部２０３に到達する。アドレス変換処理部２０３の内側ＮＩＣ受信処理部５０１は、ＴＣＰ ＡＣＫパケットの送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を変換する（Ｓ２５１８）。

【０１３３】

アドレス変換処理を施されたＴＣＰ ＡＣＫパケットは、ＴＣＰ／ＩＰプロトコルスタック２０５に到達する。ＴＣＰ／ＩＰプロトコルスタック２０５は、ＴＣＰ ＡＣＫパケットの到着を以て、コネクションの切断が完了したことを認識する（Ｓ２５１９）。

【０１３４】

一方、ステップＳ２５０９にてアドレス変換を行った後、アドレス変換処理部はアドレステーブル更新カウンタの値を、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０のタイマ用カウンタ値フィールドに書き込む（Ｓ２５２０）。テーブル更新処理部５０５は定期的に内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０のカウンタ値フィールドを監視し、所定時間が経過したら、内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０の該当レコードを削除する（Ｓ２５２１、Ｓ２５２２）。

【０１３５】

なお、ＴＣＰコネクションを切断する手段は、ＴＣＰ　ＦＩＮパケットだけではない。アプリケーションプログラムのフリーズ等、異常な状態に陥った時にＴＣＰコネクションを強制的に切断するために、ＴＣＰ　ＲＳＴパケットが存在する。ＴＣＰ　ＲＳＴパケットが発生した際の切断シーケンスは、図２５、図２６及び図２７の点線で囲った範囲の処理が変わることとなるが、詳細は割愛する。

【０１３６】

［まとめ］

ＸＰＴＣＰ非対応ＰＣ１０２から受信したパケットＰ１４０２は、内側ＮＩＣ１０４及び外側ＮＩＣ１０８のＩＰアドレスとは無関係である。このため、パケットＰ１４０２のままでは、ＴＣＰ／ＩＰプロトコルスタック２０５が所定のパケットの処理を行うことができない。そこで、一旦内側ＮＩＣアドレステーブル２０９のレコードに、パケットＰ１４０２に付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号をメモしておく。更に、後で書き戻すために索引となるポート番号を連番で付与する。そして、ＴＣＰ／ＩＰプロトコルスタック２０５がパケットの受信処理ができるようにするために、パケットＰ１４０２を「第一仮ＩＰアドレスを有する架空のホストから、内側ＮＩＣのＩＰアドレスに向けて送信されたパケット」とする、パケットＰ１４０５に書き換える。

【０１３７】

なお、この時、送信元ポート番号には索引ＰＯＲＴを付与し、宛先ポート番号は敢えて変更しない。殆どの場合、宛先ポート番号は周知のウェルノウンポート（well known port）と呼ばれる特定のポート番号である。また、ＸＰＴＣＰも特定のサービスに向けて実装している。ＸＰＴＣＰはサービス毎に異なった暗号化処理を施す必要があり、宛先ポート番号でサービスを区別しなければならないので、内側ＮＩＣ受信処理部５０１はパケッ

トに付されている送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える際、宛先ポート番号だけは変更しない。

【０１３８】

以上説明したように、ＸＰＴＣＰゲートウェイ装置１０１は、受信したパケットを一旦内部のＴＣＰ／ＩＰプロトコルスタック２０５が扱えるように、受信したパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換える。そして、送信する直前に再度送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き戻す。このため、ＸＰＴＣＰゲートウェイ装置１０１は既存のネットワーク環境に全く設定の変更を要することなく、単に通信経路上にＸＰＴＣＰゲートウェイ装置１０１を挟み込むように接続するだけで、容易にＸＰＴＣＰ機能を提供することができる。

【０１３９】

更に副次的効果として、ＸＰＴＣＰゲートウェイ装置１０１に接続されるあらゆる端末やサーバからは、ＸＰＴＣＰゲートウェイ装置１０１を認識することができない。ＰＩＮＧ等のＩＣＭＰパケットすらそのまま転送されてしまうので、ＸＰＴＣＰゲートウェイ装置１０１はネットワーク的に全く見えない装置として作用する。

【０１４０】

そして更に副次的効果として、ＸＰＴＣＰゲートウェイ装置１０１の内側ＮＩＣ１０４及び外側ＮＩＣ１０８に設定するＩＰアドレスは、ＸＰＴＣＰゲートウェイ装置１０１に接続されるあらゆるホストと干渉しない。つまり、内側ＮＩＣ１０４及び外側ＮＩＣ１０８に設定するＩＰアドレスは、ＸＰＴＣＰゲートウェイ装置１０１が接続されるサブネットとは一切関係の無いＩＰアドレスを設定しても、或は接続されるホストと重複するＩＰアドレスであっても全く問題がない。全てのパケットはＸＰＴＣＰゲートウェイ装置１０１内部でアドレス変換が施され、送信される際にはアドレスが書き戻されるので、内側ＮＩＣ１０４及び外側ＮＩＣ１０８に設定するＩＰアドレスはネットワークの外に現れない。内側ＮＩＣ１０４及び外側ＮＩＣ１０８に設定するＩＰアドレスは、ループバックアドレスやマルチキャストアドレス等の特殊なものを除いて、何を設定してもよいのである。

【０１４１】

［応用例］

本実施形態に係るＸＰＴＣＰゲートウェイ装置１０１は、以下のような応用例が考えられる。

（１）ＸＰＴＣＰゲートウェイ装置１０１は、容易にサーバ機能を実装することができる。例えば、ＸＰＴＣＰ処理対象マスタを編集するためのユーザインターフェースを提供するためにｗｅｂサーバプログラムを稼働させて、予め特定のポート番号に対応しておく。一例として、１００３０というポート番号を用いるとする。

ＸＰＴＣＰ処理部２０６は、宛先ポート番号がこの１００３０であった場合、暗号化処理を施すことなく、そのままｗｅｂサーバプログラムに引き渡す。このようにＸＰＴＣＰ処理部２０６を構成することで、ＸＰＴＣＰゲートウェイ装置１０１は容易にサーバ機能を実装できる。

【０１４２】

（２）アドレス変換処理部２０３が、内側ＮＩＣアドレステーブル２０９と外側ＮＩＣアドレステーブル２１０の、二つのテーブルで送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える実装形態であることには理由がある。

外側ＮＩＣアドレステーブル２１０の、宛先ＩＰアドレスフィールドを書き換えると、端末が意図しているＩＰアドレスとは別のＩＰアドレスのサーバと通信することができる。

図２８は、ＸＰＴＣＰゲートウェイ装置１０１において、送信するパケットの宛先ＩＰアドレスを書き換える応用形態を説明する概略図である。

端末２８０１には「Ａ」というＩＰアドレスが付与されている。今、端末２８０１は「Ｂ」というＩＰアドレスが付与されているサーバ２８０２に接続しようと、パケットＰ２

８０３を送信したとする。パケットＰ２８０３の送信元ＩＰアドレスは「Ａ」であり、宛先ＩＰアドレスは「Ｂ」である。
ＸＰＴＣＰゲートウェイ装置１０１の内側ＮＩＣアドレステーブル２０９は、「Ａ」と「Ｂ」という対応関係を忠実に再現できる必要があるので、そのままのＩＰアドレスが記録される。

【０１４３】
しかし、外側ＮＩＣアドレステーブル２１０は、「Ａ」と「Ｂ」という対応関係を必ずしも忠実に再現できていなくてもよい。今、宛先ＩＰアドレスを「Ｃ」に書き換えると、ＸＰＴＣＰゲートウェイ装置１０１から送出されるパケットＰ２８０４は、送信元ＩＰアドレスが「Ａ」であり、宛先ＩＰアドレスが「Ｃ」になる。すると、パケットＰ２８０４はＩＰアドレスが「Ｃ」のサーバ２８０５に到達する。
このように、ＸＰＴＣＰゲートウェイ装置１０１は、外側ＮＩＣアドレステーブル２１０に登録されている宛先ＩＰアドレスを書き換えることで、宛先ＩＰアドレスを端末２８０１が把握していない先で変換することができる。この動作を応用すると、ＸＰＴＣＰゲートウェイ装置１０１を二台以上数珠繋ぎに構成することで、容易にＶＰＮ（Vitual Private Network）を構築できる。

【０１４４】
（３）アドレス変換処理部２０３が、内側ＮＩＣアドレステーブル２０９と外側ＮＩＣアドレステーブル２１０の、二つのテーブルで送信元及び宛先ＭＡＣアドレス、ＩＰアドレス及びポート番号を書き換える実装形態であることには理由がある。
外側ＮＩＣアドレステーブル２１０の、送信元ＩＰアドレスフィールドを書き換えると、サーバの側に存在する悪意ある第三者から、端末２８０１の本当のＩＰアドレスを隠蔽することができる。
図２９は、ＸＰＴＣＰゲートウェイ装置１０１において、送信するパケットの送信元ＩＰアドレスを書き換える応用形態を説明する概略図である。
端末２９０１には「Ａ」というＩＰアドレスが付与されている。今、端末２９０１は「Ｂ」というＩＰアドレスが付与されているサーバ２９０２に接続しようと、パケットＰ２９０３を送信したとする。パケットＰ２９０３の送信元ＩＰアドレスは「Ａ」であり、宛先ＩＰアドレスは「Ｂ」である。
ＸＰＴＣＰゲートウェイ装置１０１の内側ＮＩＣアドレステーブル２０９は、「Ａ」と「Ｂ」という対応関係を忠実に再現できる必要があるので、そのままのＩＰアドレスが記録される。

【０１４５】
しかし、外側ＮＩＣアドレステーブル２１０は、「Ａ」と「Ｂ」という対応関係を必ずしも忠実に再現できていなくてもよい。今、送信元ＩＰアドレスを「Ｄ」に書き換えると、ＸＰＴＣＰゲートウェイ装置１０１から送出されるパケットＰ２９０４は、送信元ＩＰアドレスが「Ｄ」であり、宛先ＩＰアドレスが「Ｂ」になる。すると、サーバ２９０２から見るとあたかも送信元ＩＰアドレスが「Ｄ」の仮想端末２９０５から送信されたように見えるので、ＩＰアドレス「Ａ」の端末２９０１の存在を隠蔽することができる。
このように、ＸＰＴＣＰゲートウェイ装置１０１は、外側ＮＩＣアドレステーブル２１０に登録されている送信元ＩＰアドレスを書き換えることで、送信元ＩＰアドレスを悪意ある第三者から隠蔽することができる。

【０１４６】
（４）暗号化処理部１００５は、ＴＣＰ／ＩＰプロトコルスタック２０５がＴＣＰデータパケットからペイロード部分を取り出して復元したストリームデータに対して、暗号化処理を施す。この暗号化処理は、必ずしもストリームデータ全体を暗号化するとは限らない。
例えば、周知のＴＥＬＮＥＴ（ＴＣＰポート２３番）の場合は、ストリームデータを全て暗号化する必要がある。
しかし、例えば周知のＳＭＴＰ（Simple Mail Transfer Protocol：ＴＣＰポート２５

番）の場合は、送信したメールがＳＭＴＰサーバを転々と転送される可能性がある。その際、全てのＳＭＴＰサーバがＸＰＴＣＰの認証及び暗号化処理に対応することは困難である。そこで、送信元の端末と、最終的に受信する側のホストのみ認証及び暗号化処理に対応させ、暗号化の対象はＳＭＴＰメッセージの本文のみとする。周知のように、ＳＭＴＰメッセージは一行の空改行をセパレータとしてヘッダと本文に分けられ、ヘッダにはメールがＳＭＴＰサーバ等のホストを経由する際に記録される情報（Ｒｅｃｅｉｖｅｄ：ヘッダ）が追記される。

本実施形態の暗号化処理部１００５も、ＳＭＴＰやＨＴＴＰ等、ストリームデータがヘッダと本文とに分離できるプロトコルの場合等、プロトコルに応じて暗号化の対象をストリームデータ全部ではなく本文のみとする、といった処理が含まれることが好ましい。

【０１４７】

本実施形態では、ネットワークゲートウェイ装置を開示した。

既存のネットワークＯＳに標準搭載されているＴＣＰ／ＩＰプロトコルスタック２０５の機能を最大限有効に活用しつつ、必要最小限のプログラムを追加することでＸＰＴＣＰゲートウェイ装置１０１を実現するために、ＴＣＰ／ＩＰプロトコルスタック２０５を「騙す」処理を施す。ＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレスとは無関係である筈のパケットをＴＣＰ／ＩＰプロトコルスタック２０５が処理できるようにするために、予めパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を内側ＮＩＣアドレステーブル２０９及び外側ＮＩＣアドレステーブル２１０にメモしておく。その上で、受信したパケットに付されている送信元ＭＡＣアドレス及び送信元ＩＰアドレスは偽のＭＡＣアドレス及び偽のＩＰアドレスに、宛先ＭＡＣアドレス及び宛先ＩＰアドレスはＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレス及びＭＡＣアドレスに書き換えてから、ＴＣＰ／ＩＰプロトコルスタック２０５に与える。

【０１４８】

更に、パケットを本来の送信先へ送信する際には、ＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレス及びＭＡＣアドレスから偽のＭＡＣアドレス及び偽のＩＰアドレスに返送するように、ＴＣＰ／ＩＰプロトコルスタック２０５を騙し、ＴＣＰ／ＩＰプロトコルスタック２０５から送信されるパケットの送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを先に書換テーブルにメモした本来のアドレスに書き戻して、本来の送信先へ送信する。

【０１４９】

このようにＸＰＴＣＰゲートウェイ装置１０１は、受信したパケットを一旦内部のＴＣＰ／ＩＰプロトコルスタック２０５が扱えるように、受信したパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き換える。そして、送信する直前に再度送信元ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＭＡＣアドレス及び宛先ＩＰアドレスを書き戻す。このため、ＸＰＴＣＰゲートウェイ装置１０１は既存のネットワーク環境に全く設定の変更を要することなく、単に通信経路上にＸＰＴＣＰゲートウェイ装置１０１を挟み込むように接続するだけで、容易にＸＰＴＣＰ機能を提供することができる。

【０１５０】

以上、本発明の実施形態例について説明したが、本発明は上記実施形態例に限定されるものではなく、特許請求の範囲に記載した本発明の要旨を逸脱しない限りにおいて、他の変形例、応用例を含む。

【符号の説明】

【０１５１】

１０１…ＸＰＴＣＰゲートウェイ装置、１０２…ＸＰＴＣＰ非対応ＰＣ、１０３…ＸＰＴＣＰ非対応ＰＣ、１０４…内側ＮＩＣ、１０５…ＸＰＴＣＰ非対応ＰＣ、１０６…ＸＰＴＣＰ対応ＰＣ、１０７…ＸＰＴＣＰ対応サーバ、１０８…外側ＮＩＣ、１０９…ＸＰＴＣＰ非対応ネットワーク、１１０…ＸＰＴＣＰ対応ネットワーク、２０１…初期設定部、

２０２…ネットワーク設定情報メモリ、２０３…アドレス変換処理部、２０４…仮ＩＰＭＡＣリスト、２０５…ＴＣＰ／ＩＰプロトコルスタック、２０６…ＸＰＴＣＰ処理部、２０７…ソケット処理部、２０８…ＸＰＴＣＰ処理対象マスタ、２０９…内側ＮＩＣアドレステーブル、２１０…外側ＮＩＣアドレステーブル、２１１…ＸＰＴＣＰポリシーテーブル、２１２…ＴＣＰポート番号メモリ、２１３…アドレステーブル更新カウンタ、４０１…ＩＰヘッダ、４０２…ＭＡＣヘッダ、４０３…ＴＣＰヘッダ、４０４…ＵＤＰヘッダ、５０１…内側ＮＩＣ受信処理部、５０２…外側ＮＩＣ受信処理部、５０３…外側ＮＩＣ送信処理部、５０４…内側ＮＩＣ送信処理部、５０５…テーブル更新処理部、５０６…ポリシー回答部、６０１…受信パケット判定部、６０２…アドレス置換部、６０３…コネクション登録処理部、６０４…レコード削除準備処理部、６０５…削除予定リスト、７０１…受信パケット判定部、７０２…アドレス置換部、７０３…レコード削除処理部、８０１…送信パケット判定部、８０２…ＡＲＰ応答処理部、８０３…動的ポート記録処理部、８０４…アドレス復元部、９０１…送信パケット判定部、９０２…アドレス復元部、１００１…イベント検出部、１００２…ソケット操作部、１００３…ポリシー設定部、１００４…ソケットメモリ領域、１００５…暗号化処理部、１００６…復号処理部、２８０１…端末、２８０２…サーバ、２８０５…サーバ、２９０１…端末、２９０２…サーバ、２９０５…仮想端末

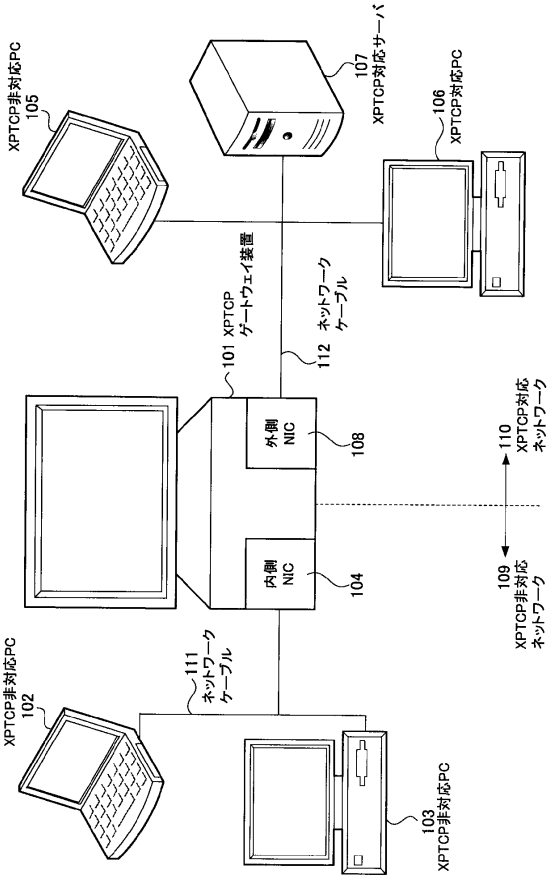
【要約】

【課題】既存のネットワーク環境に対して設定変更を何ら強いることなく、容易にセキュリティを高めた暗号化通信機能を追加できるネットワークゲートウェイ装置を提供する。

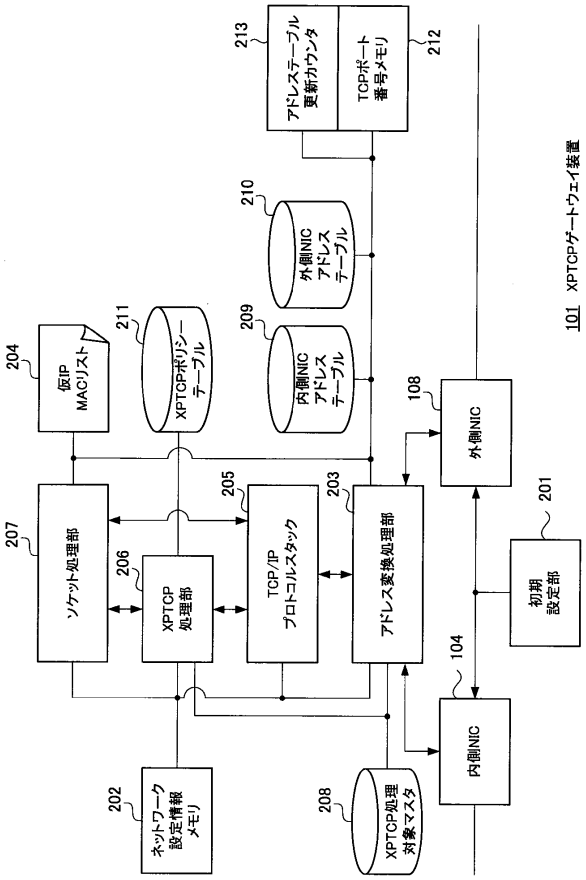
【解決手段】ＴＣＰ／ＩＰプロトコルスタック２０５の機能を最大限有効に活用しつつ、必要最小限のプログラムを追加することでＸＰＴＣＰゲートウェイ装置１０１を実現するために、ＴＣＰ／ＩＰプロトコルスタック２０５を「騙す」処理を施す。ＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレスとは無関係である筈のパケットをＴＣＰ／ＩＰプロトコルスタック２０５が処理できるようにするために、予めパケットに付されている送信元ＭＡＣアドレス、送信元ＩＰアドレス、送信元ポート番号、宛先ＭＡＣアドレス、宛先ＩＰアドレス及び宛先ポート番号を書換テーブルにメモしておく。その上で、受信したパケットに付されている送信元ＭＡＣアドレス及び送信元ＩＰアドレスは偽のＭＡＣアドレス及び偽のＩＰアドレスに、宛先ＭＡＣアドレス及び宛先ＩＰアドレスはＸＰＴＣＰゲートウェイ装置１０１に割り当てられているＩＰアドレス及びＭＡＣアドレスに書き換えてから、ＴＣＰ／ＩＰプロトコルスタック２０５に与える。

【選択図】図２

【図１】



【図２】



【図３】

209 内側NICアドレステーブル

プロトコル種別(TCP/UDP)
送信元MACアドレス
送信元IPアドレス
送信元ポート番号
宛先MACアドレス
宛先IPアドレス
宛先ポート番号
索引用ポート番号
タイマ用カウンタ値

210 外側NICアドレステーブル

プロトコル種別(TCP/UDP)
送信元MACアドレス
送信元IPアドレス
送信元ポート番号
宛先MACアドレス
宛先IPアドレス
宛先ポート番号
索引用ポート番号
動的ポート番号
タイマ用カウンタ値

211 XPTCPポリシーテーブル

プロトコル種別(TCP/UDP)
索引用ポート番号
レコード番号

202 ネットワーク設定情報メモリ

内側NICMACアドレス
内側NICIPアドレス
外側NICMACアドレス
外側NICIPアドレス

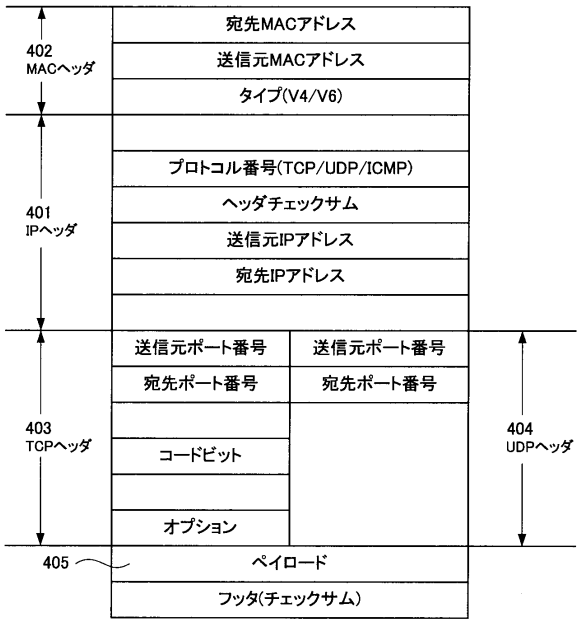
204 仮IPMACリスト

内側NICIPアドレス
第一仮MACアドレス
第一仮IPアドレス
外側NICIPアドレス
第二仮MACアドレス
第二仮IPアドレス

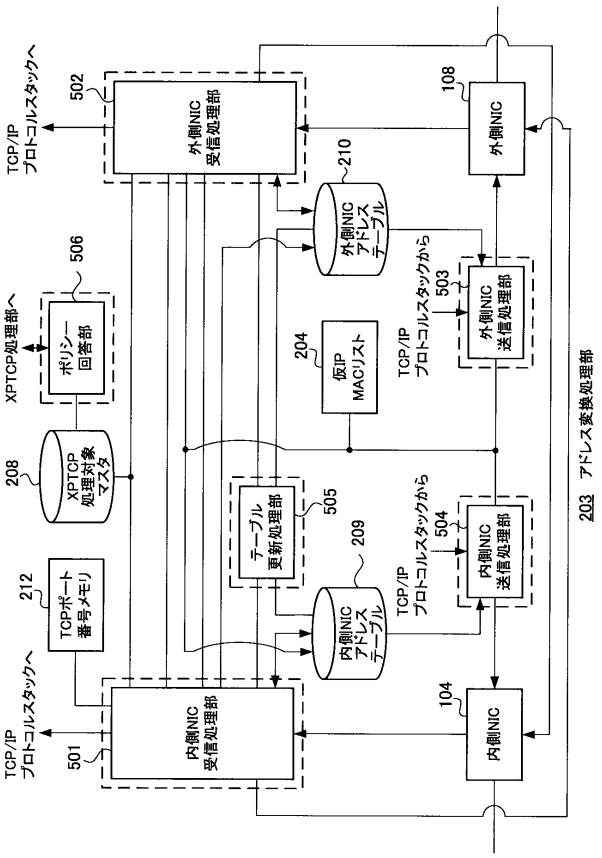
208 XPTCP処理対象マスタ

レコード番号
プロトコル種別(TCP/UDP)
送信元IPアドレス
送信元ポート番号
宛先IPアドレス
宛先ポート番号
暗号種別他

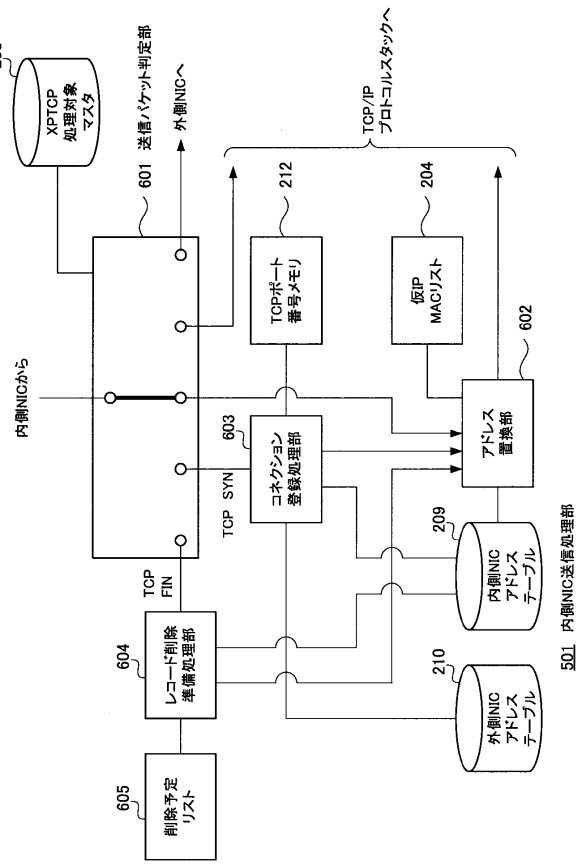
【図４】



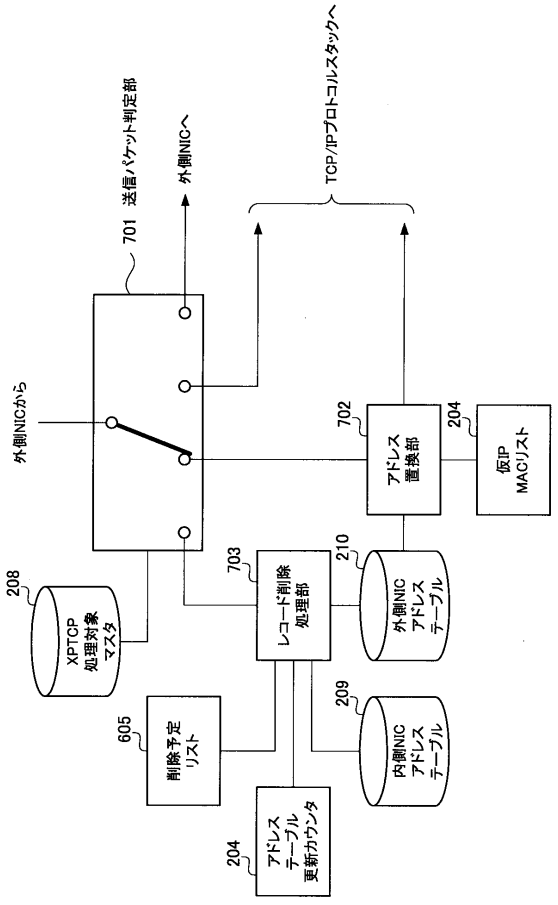
【図５】


TCP/IP プロトコルスタックへ
502 外側NIC 受信処理部
108 外側NIC
210 外側NIC アドレス テーブル
XPTCP処理部へ
506 ポリシー 回答部
503 外側NIC 送信処理部
TCP/IP プロトコルスタックから
204 仮IP MACリスト
208 XPTCP 処理対象 マスタ
テーブル 更新処理部 505
209 内側NIC アドレス テーブル
504 内側NIC 送信処理部
212 TCPポート 番号メモリ
104 内側NIC
501 内側NIC 受信処理部
203 アドレス変換処理部

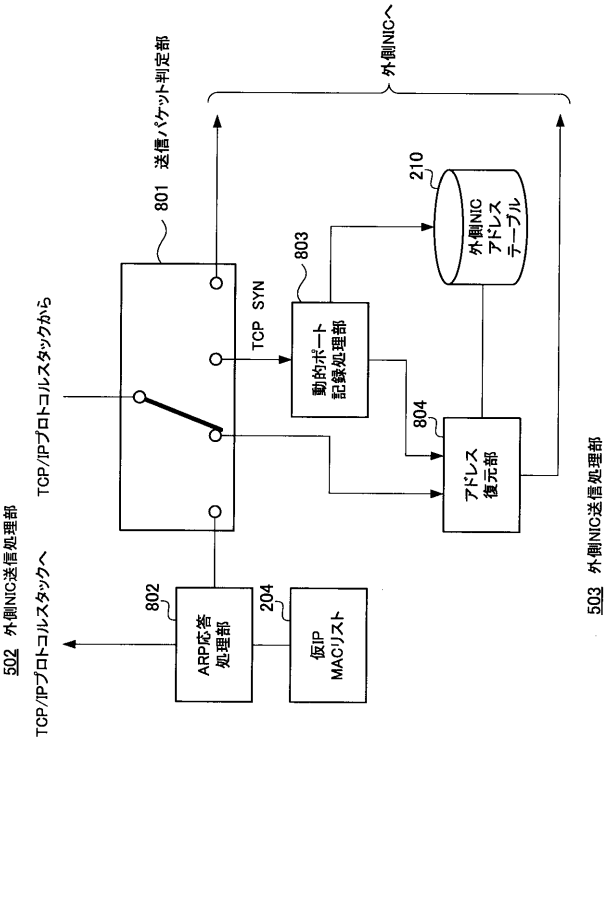
【図６】


208 XPTCP 処理対象 マスタ
601 送信パケット判定部
外側NICへ
TCP/IP プロトコルスタックへ
内側NICから
212 TCPポート 番号メモリ
204 仮IP MACリスト
TCP SYN
603 コネクション 登録処理部
602 アドレス 置換部
209 内側NIC アドレス テーブル
TCP FIN
604 レコード削除 準備処理部
210 外側NIC アドレス テーブル
605 削除予定 リスト
501 内側NIC送信処理部

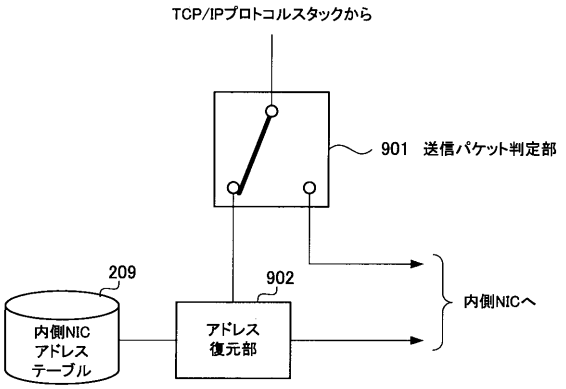
【図７】


外側NICから
701 送信パケット判定部
外側NICへ
TCP/IPプロトコルスタックへ
208 XPTCP 処理対象 マスタ
703 レコード削除 処理部
210 外側NIC アドレス テーブル
702 アドレス 置換部
204 仮IP MACリスト
605 削除予定 リスト
209 内側NIC アドレス テーブル
204 アドレス テーブル 更新カウンタ
502 外側NIC送信処理部

【図８】

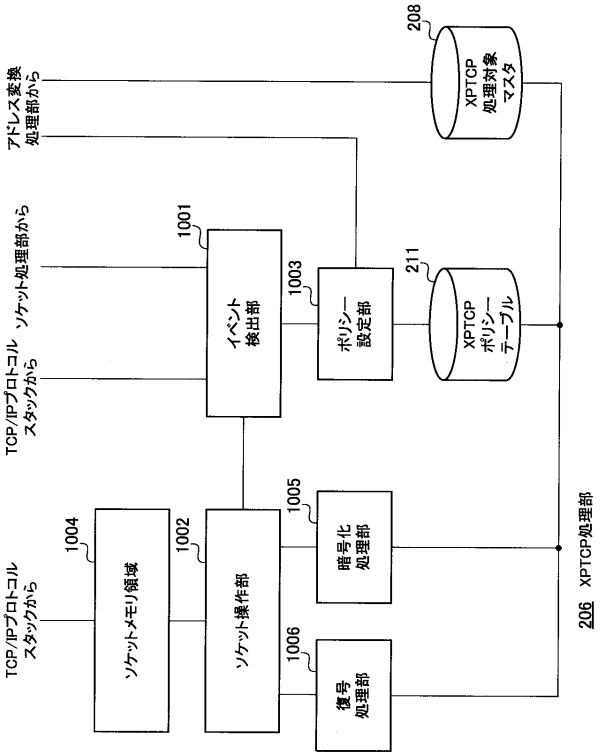

外側NICへ
801 送信パケット判定部
TCP/IPプロトコルスタックから
TCP SYN
803 動的ポート 記録処理部
210 外側NIC アドレス テーブル
804 アドレス 復元部
802 ARP応答 処理部
204 仮IP MACリスト
TCP/IPプロトコルスタックへ
503 外側NIC送信処理部

【図９】

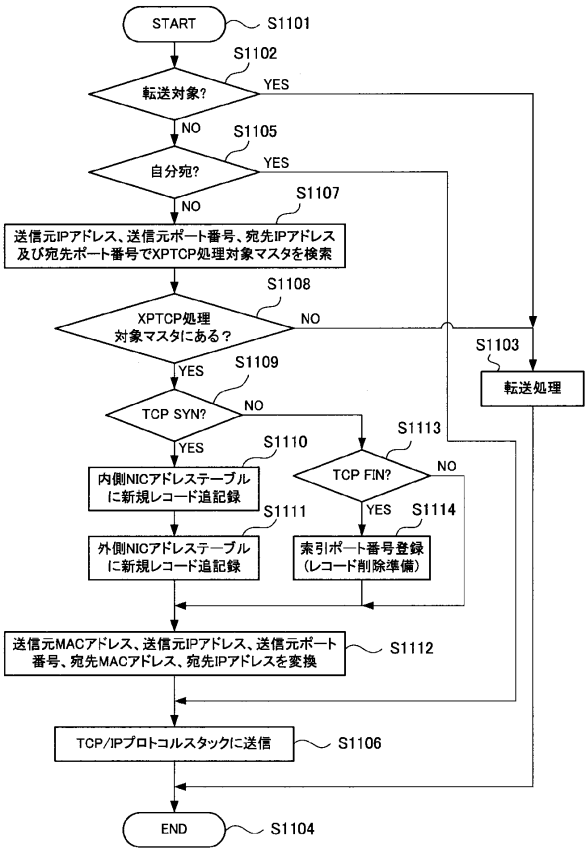


504 内側NIC送信処理部

【図１０】

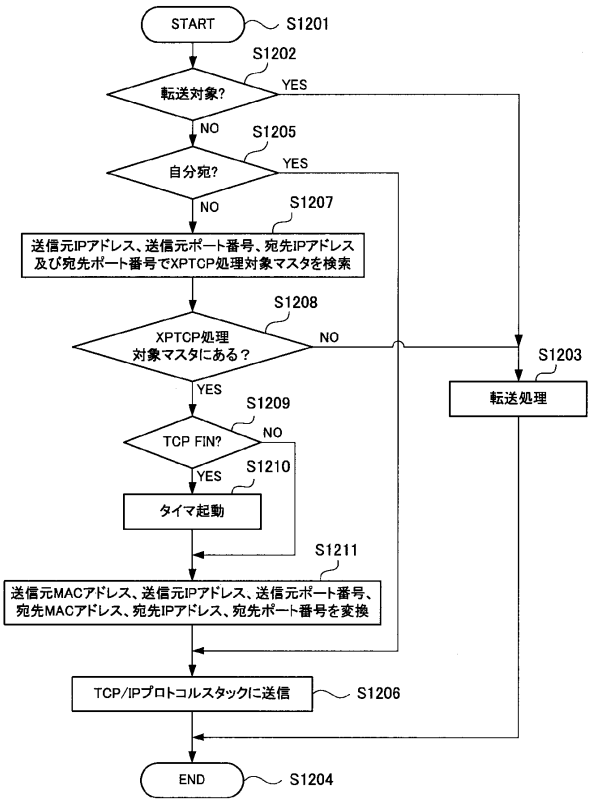


【図１１】



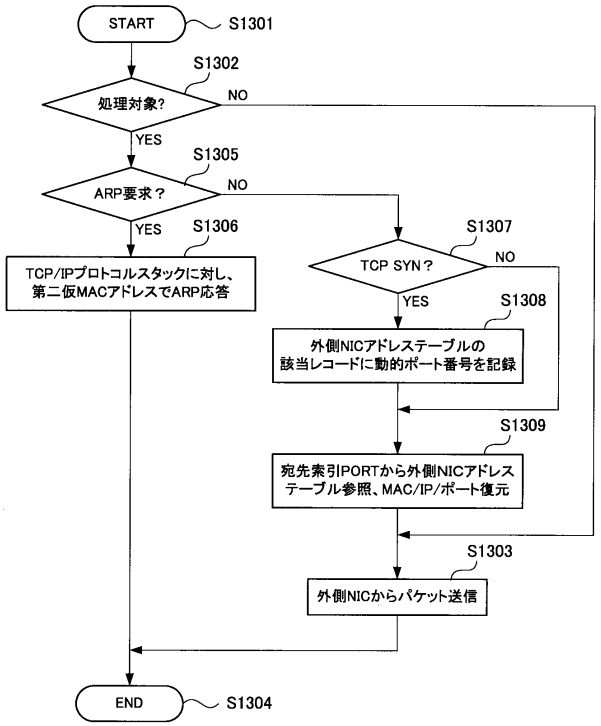
(アドレス変換処理部)内側NICパケット受信処理

【図１２】



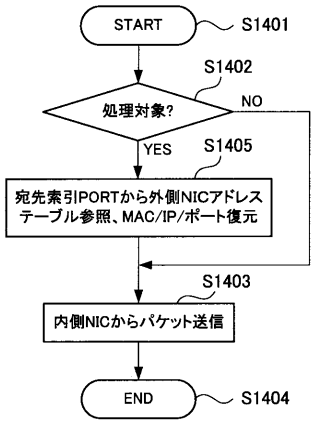
(アドレス変換処理部)外側NICパケット受信処理

【図１３】



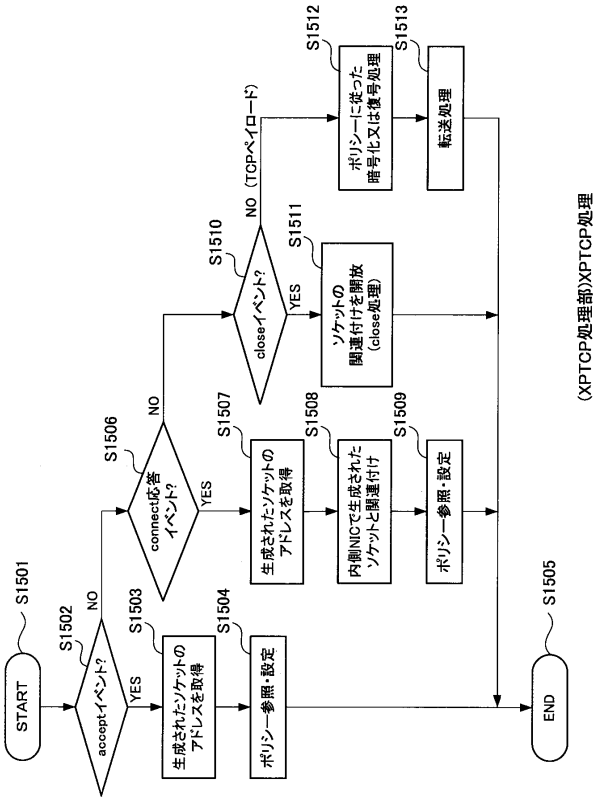
(アドレス変換処理部)外側NICパケット送信処理

【図１４】



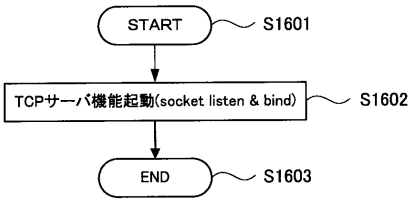
(アドレス変換処理部)内側NICパケット送信処理

【図１５】



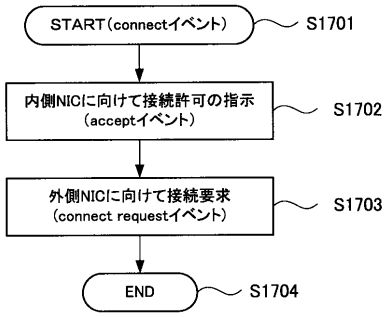
(XPTCP処理部)XPTCP処理

【図１６】



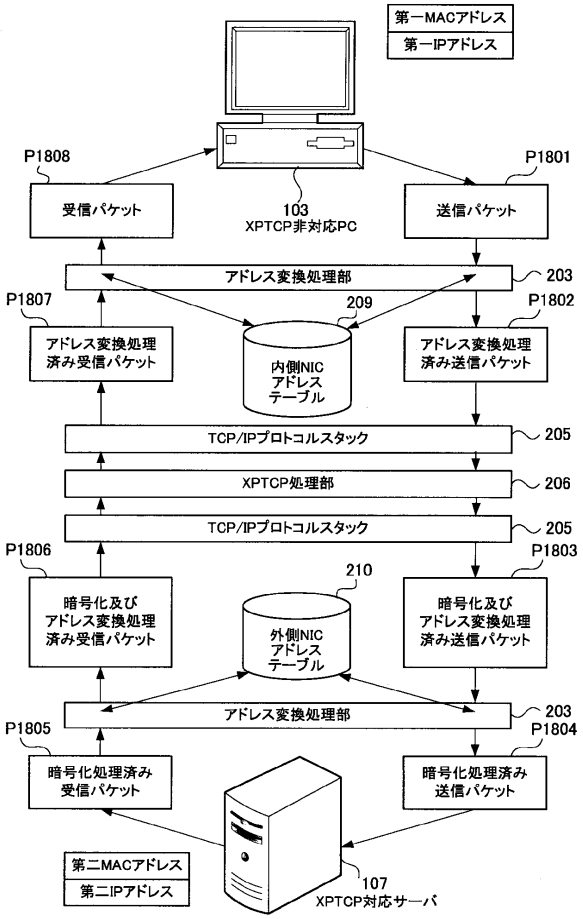
(ソケット処理部)初期処理

【図１７】

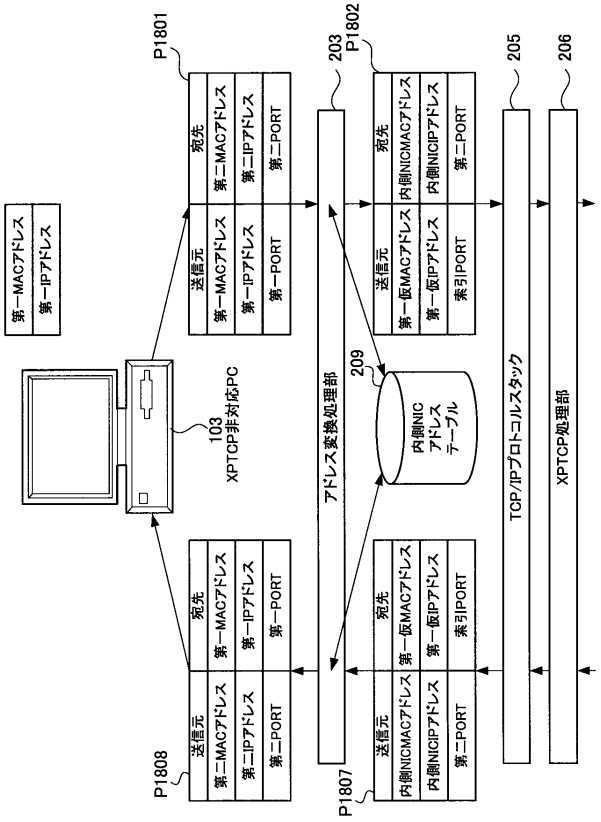


(ソケット処理部)接続要求転送理

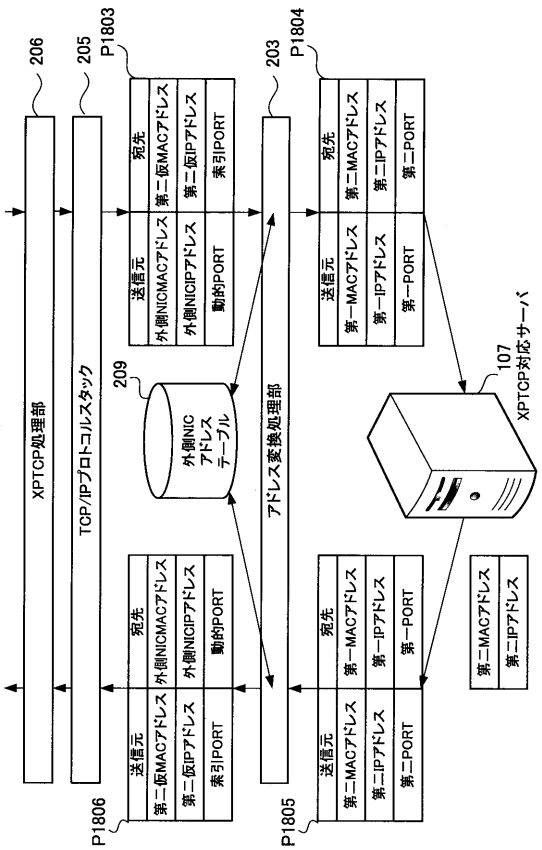
【図１８】



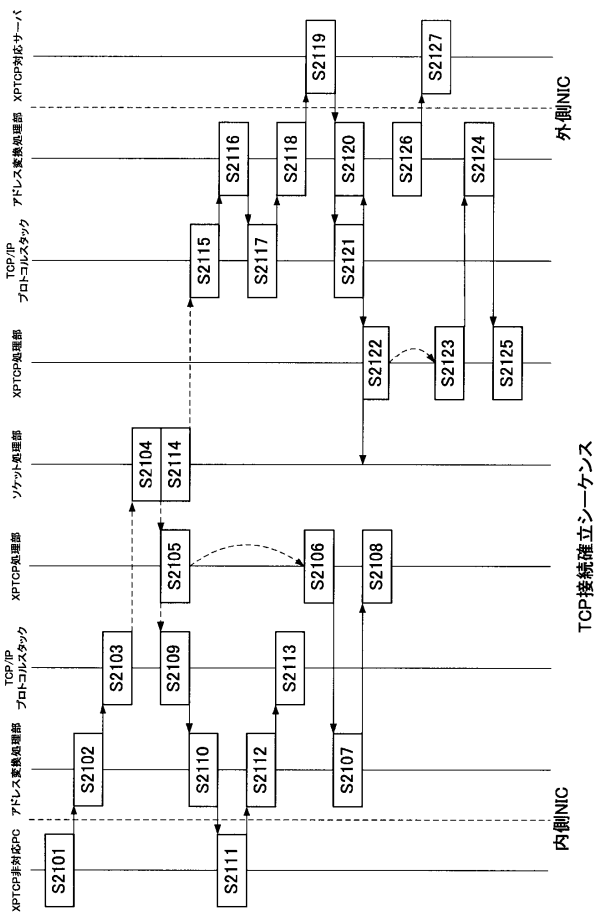
【図１９】



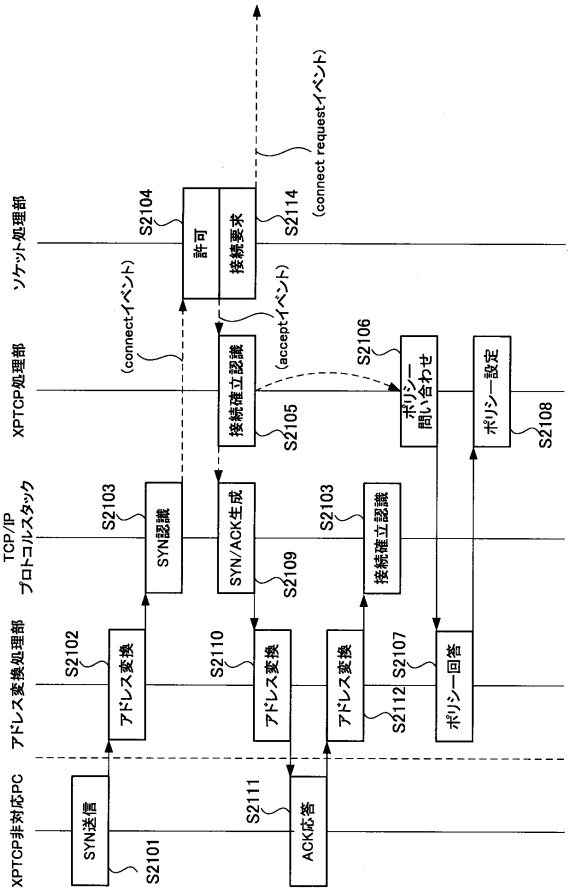
【図２０】



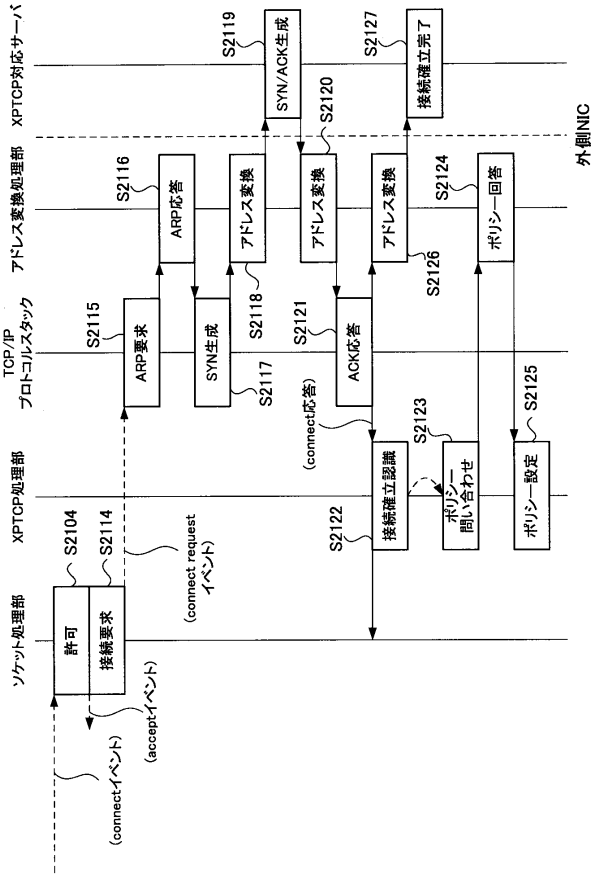
【図２１】



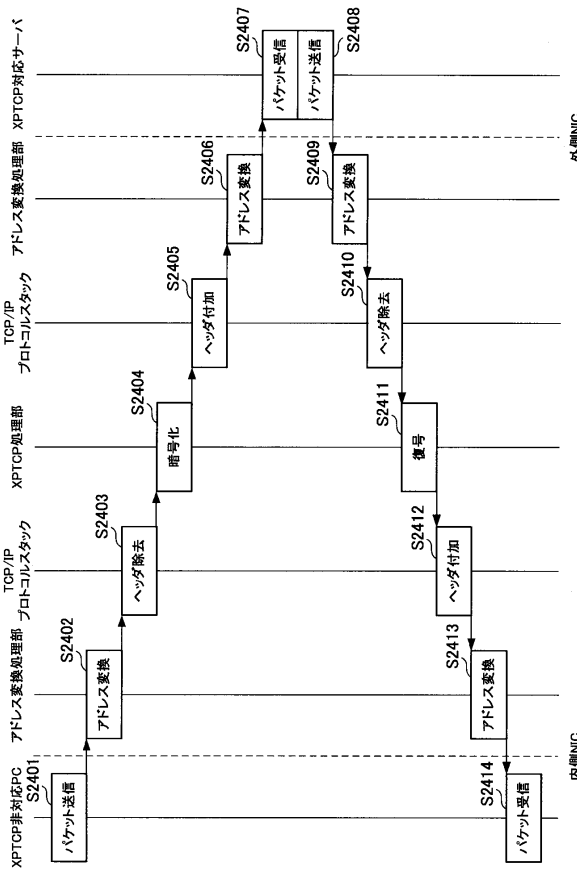
【図２２】



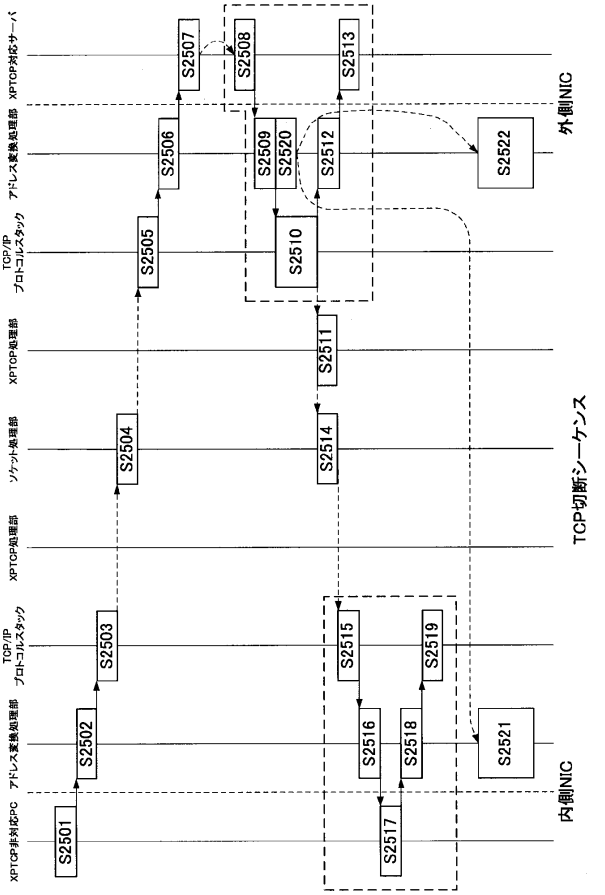
【図２３】



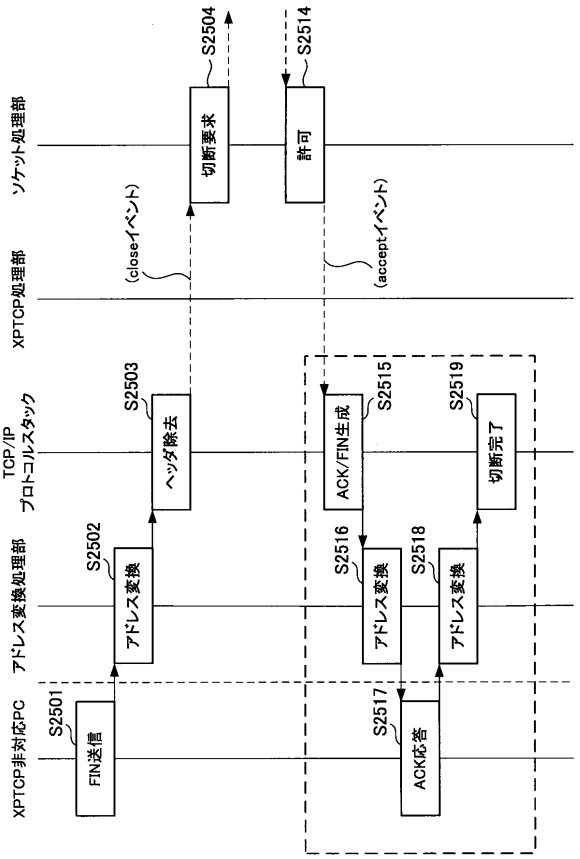
【図２４】



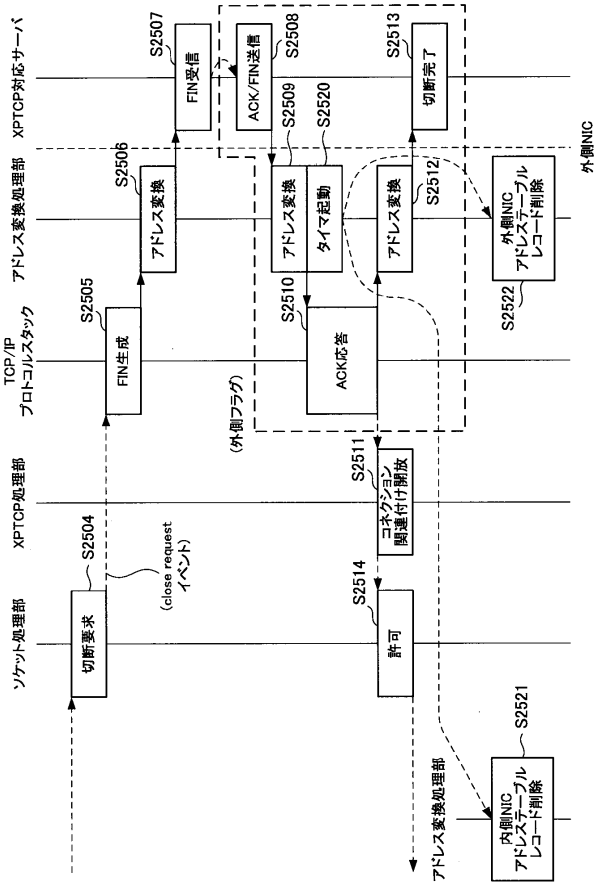
【図２５】



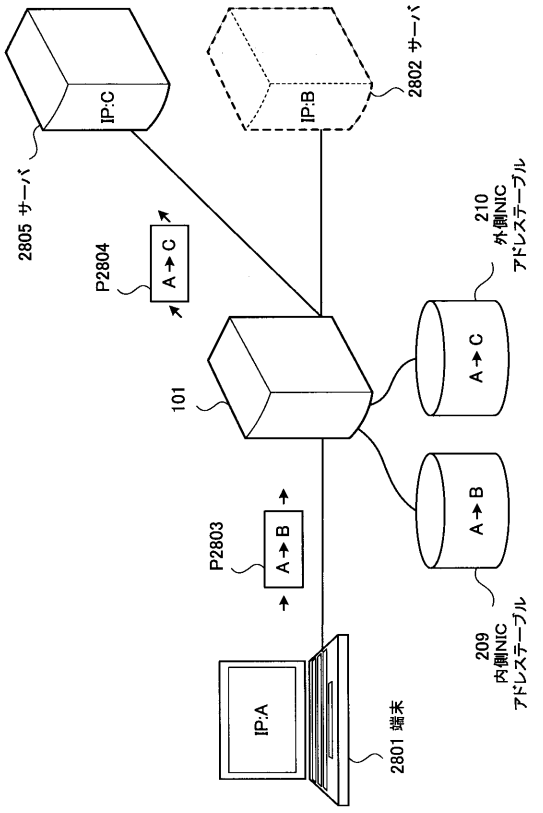
【図２６】



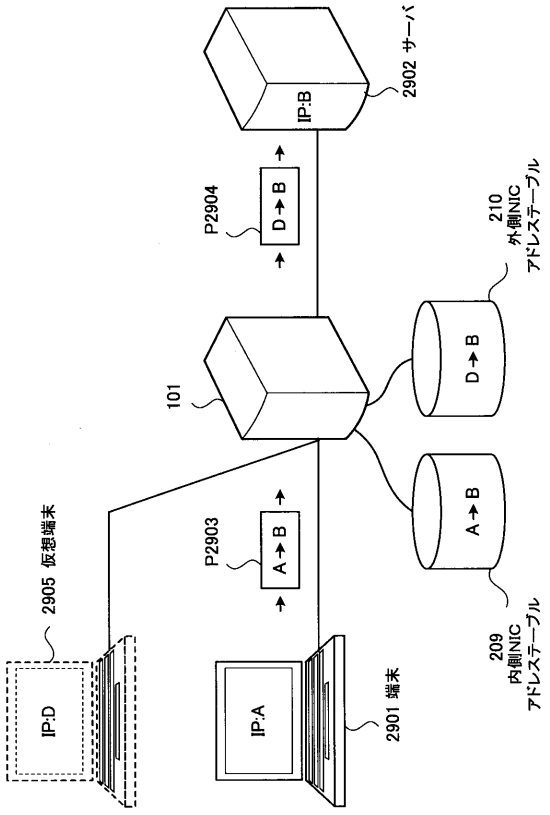
【図２７】



【図２８】



【図２９】



フロントページの続き

(56)参考文献 特許第３７８３１４２（ＪＰ，Ｂ１）
国際公開第２００５／０１５８２７（WO，Ａ１）
特開２００７－３２４７２６（ＪＰ，Ａ）
特開２００７－３２３１７２（ＪＰ，Ａ）
特開２００７－３２４７２７（ＪＰ，Ａ）
特開２００７－３３６４０１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／２８－４６
Ｈ０４Ｌ ９／１４