(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3947521号
(P3947521)
(45)発行日　平成19年7月25日(2007.7.25)　(24)登録日　平成19年4月20日(2007.4.20)

(51)Int.Cl.　F I
H04L 29/06 (2006.01)　H04L 13/00　305A

請求項の数 6　(全 24 頁)

(21)出願番号　特願2003-573850(P2003-573850)
(86)(22)出願日　平成14年3月5日(2002.3.5)
(86)国際出願番号　PCT/JP2002/002001
(87)国際公開番号　WO2003/075537
(87)国際公開日　平成15年9月12日(2003.9.12)
審査請求日　平成16年6月14日(2004.6.14)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100090011
弁理士　茂泉　修司
(72)発明者　城田　克也
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内
(72)発明者　島村　彰
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内

最終頁に続く

(54)【発明の名称】通信装置

(57)【特許請求の範囲】
【請求項１】
受信パケットに含まれるプロトコル属性を検出し、該プロトコル属性に基づいてプロトコル処理順序を示すプロトコル処理順序データを生成するプロトコル処理順序データ生成部と、
該プロトコル処理順序データに基づき該受信パケット中の複数のプロトコルを個別に処理するプロトコル変換部とを備え、
該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを先頭から順次該プロトコル処理部で処理させるヘッダ識別部と、該プロトコル処理部でのプロトコル処理回数をカウントするカウンタとを備え、該ヘッダ識別部は、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了することを特徴とした通信装置。
【請求項２】
請求項１において、
該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを先頭から順次該プロトコル処理部で処理させるヘッ

ダ処理部と、該ヘッダ識別部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了させる処理完了部とを備えていることを特徴とした通信装置。

【請求項３】

請求項１において、

該プロトコル処理順序データがプロトコル総処理回数を含んでおり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該受信パケットを待機させるデータ待機部と、該プロトコル処理順序データに基づいて該データ待機部における受信パケット中のプロトコルを該プロトコル処理部で先頭から順次処理させると共に、該プロトコル処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が該プロトコル総処理回数に達したときプロトコル処理を終了させる処理順序制御部とを備えていることを特徴とした通信装置。

【請求項４】

請求項１において、

該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させるヘッダ識別部と、該プロトコル処理部でのプロトコル処理回数をカウントするカウンタとを備え、該ヘッダ識別部は、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了することを特徴とした通信装置。

【請求項５】

請求項１において、

該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させるヘッダ処理部と、該ヘッダ処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了させる処理完了部とを備えていることを特徴とした通信装置。

【請求項６】

請求項１において、

該プロトコル処理順序データが該プロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んでおり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該受信パケットを待機させるデータ待機部と、該プロトコル処理順序データに基づいて該データ待機部における受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させると共に、該プロトコル処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が該プロトコル総処理回数に達したときプロトコル処理を終了させる処理順序制御部とを備えていることを特徴とした通信装置。

【発明の詳細な説明】

【０００１】

【技術分野】

【０００２】

本発明は通信装置に関し、特に通信プロトコルを用いてデータの送受信を行う通信装置に関するものである。

【０００３】

プロトコルとは通信方法を定めた規約のことであり、全7層のOSI参照モデルによって構成されている。各層は、上位層から受け取った送信データに対して、各プロトコルに従っ

た処理情報をヘッダとして付加して下位層に渡す。また、下位層から受け取った受信データに対して、付加されているヘッダを抜き取り、その処理情報に従った処理を実行して上位層に渡す。

【０００４】

個々の通信装置は、それぞれ単独のプロトコルにしか対応していない。様々なプロトコルを実現する必要があるならば、それら個々のプロトコルに対応した通信装置を用意する必要がある。しかしながら、この方法では手間とコストが大幅にかかってしまう。従って、より容易にあらゆる種類のプロトコルを実現する手段が求められている。

【背景技術】

【０００５】

図18(1)は、従来からよく知られているインターネット網を介して接続される通信システムを示している。図中、10はパーソナルコンピュータ（以下、PCと略称する。）、11はL2TP Access Control（以下、LACと略称する。）、12はL2TP Network Server（以下、LNSと略称する。）であり、13は企業内網としてのLAN（Local Area Network）である。そして、LAN13には、PC14およびメールサーバとしてのPC15が設置されている。

【０００６】

このような通信システムにおいて、PC10は、パケットP1をLAN13内のPC14に送るとき、まずISP(Internet Service Provider)が提供するLAC11との間にコネクションを確立するため、ペイロードに送信元であるPC10のIPアドレス(a)、及び送信先であるPC14のIPアドレス(b)を付加したIP(a→b)フレームを生成し、これをPPP(Point To Point)プロトコルでカプセル化したパケットP1を送出する。

【０００７】

LAC11では、このコネクションから受信したPPPプロトコルパケットをさらにLNS12に送信するため、送信元であるLAC11のIPアドレス(x)及び送信先であるLNS12のIPアドレス(y)をパケットP1に付加した（IP(x→y)プロトコルでカプセル化した）パケットP2を宛先ネットワーク上のLNS12に対してインターネット網INETのトンネルを経由して送出する。

【０００８】

このパケットP2を受信したLNS12は、パケットP2からLAC11及びLNS12のIPアドレスを除去するデカプセル化を行ったパケットP3をLAN13へ送る。

【０００９】

そしてパケットP3は、LAN13を経由してメールサーバPC15に送られ、PC15はパケットP3を宛先であるPC14に転送してデータの送信が完了する。

【００１０】

従って、LNS12は、同図(2)に示すように、IP(x→y)終端処理（ステップS21）と、PPP終端処理（ステップS22）と、IP(a→b)終端処理（ステップS23）が必要となる。

【００１１】

この場合のPC10→LNS12のPPPプロトコルセッション(1)では、PC10のユーザーはISPが提供するNAS（Network Access Server）（図示せず）との間にダイヤルアップなどの手段でコネクションを張っていた。この場合、例えば海外などの遠隔地からLAN13にアクセスするときには、LAN13内のPPPサーバにダイヤルアップしなければならずコストが嵩むことになる。

【００１２】

図19は、図18におけるLACやLNSの代わりにセキュリティ・ゲートウェイSG1,SG2を用いて企業内網のLAN13aと13bとを接続したものである。この接続を行うためには、図19(1)に示すトンネルモードと、同図(2)に示すトランスポートモードとが考えられる。

【００１３】

まず、トンネルモード(1)の場合には、LAN13aにおけるアドレス(a)のPC16から、パケットP1がセキュリティ・ゲートウェイSG1に対してIP(a→b)プロトコルにより送られる。そして、セキュリティ・ゲートウェイSG1は、この受信したパケットP1に網掛で示すように暗号化を施すとともに、IP(x→y)プロトコルでカプセル化し、インターネット網INET上の

セキュリティ・アソシエーションSA1のトンネルを経由してセキュリティ・ゲートウェイSG2に送る。

【００１４】

このセキュリティ・ゲートウェイSG2では、同図(3)に示すようにまずIP(x→y)終端処理（ステップS31）を行い、さらに暗号化処理（ステップS32）を行った後、IP(x→y)プロトコルを除去した（デカプセル化した）パケットP3をLAN13bに送る。LAN13bでは、このパケットP3におけるIP(a→b)終端処理プロトコルに従い、アドレス(b)のPC14にパケットP3が送られることとなる。

【００１５】

また、トランスポートモード(2)の場合には、PC16から対向するLAN13ｂにおけるPC14に対してパケットP4が送信される。このパケットP2はセキュリティ・ゲートウェイSG1においてペイロードが暗号化処理された後、インターネットINET及びセキュリティ・ゲートウェイSG2を経由してLAN13ｂにおけるアドレス(b)のPC14に送られることとなる（セキュリティ・アソシエーションSA2）。

【００１６】

このような図19に示したセキュリティ・ゲートウェイを用いた通信システムにおいて、同図(3)に示したような処理を行うセキュリティ・アソシエーション（トンネルモード）SA1及びセキュリティ・アソシエーション（トランスポートモード）SA2に対してはこのセキュリティ・ゲートウェイSG2は対応可能であるが、その他のモードには対応することはできない。

【００１７】

これを示したのが図20である。すなわち、セキュリティ・ゲートウェイSG2に対して、図18に示したようなPC10及びLAC11をPPPセッション(1)またはL2PPセッション(2)でも接続するような場合、LAC11から来たパケットは図18に示したようにLNSとして処理する必要があり、セキュリティ・ゲートウェイSG1から来たものはセキュリティ・ゲートウェイとしてIPsec(IP security)プロトコル処理する必要がある。

【００１８】

LNSの処理としては、IP,UDP,L2TP,PPP,IPのプロトコル処理順序が必要になり（図3参照）、セキュリティ・ゲートウェイSG2では、ESP暗号解読やIPの処理順序が必要になる（同図参照）ので、固定したプロトコルしか備わっていない通信装置の場合には、これらの処理を実行することができない。

【００１９】

上記の場合には、PPPセッションやL2TPセッション並びにセキュリティ・アソシエーションモードを例に取って説明したが、カプセル化はこの他にも種々存在する。

【００２０】

図21はこのような種々のカプセル化例を示したものである。同図(1)は標準的なイーサネットのプロトコル、同(2)はモバイル端末や基地局などにおけるイーサネットのプロトコル、同(3)はPPPoE(ADSL等)に用いるプロトコル、同(4)及び(5)はL2.5のイーサネットにMPLS(Multiprotocol Label Switching)を組み合わせたプロトコルである。

【００２１】

さらに同図(6)は、MACレイヤでのトンネリングを行うためのプロトコル、同(7)はL2TPプロトコル、同(8)は認証化（トンネルモード）を行うためのプロトコル、同(9)は認証化（トランスポートモード）を行うためのプロトコル、同(10)は暗号化（トンネルモード）を行うためのプロトコル、同(11)は暗号化（トランスポートモード）を行うためのプロトコル、同(12)は鍵交換を示すプロトコル、同(13)はIPレイヤでのトンネリングを行うためのプロトコル、同(14)はIPv4網でのIPv6でのトンネリングを行うためのプロトコル、同(15)は、IPv6拡張ヘッダなどのプロトコル、同(16)はグローバルアドレス/プライベートアドレスのトンネリングを行うためのプロトコル、そして、同(17)はIPv6網でのIPv4のトンネリングを行うためのプロトコルである。

【００２２】

このような種々のカプセル化されたパケットが入力された従来の通信装置においては、固定したプロトコルしか備えていないので、フレキシブルに対応することができないこととなる。

【００２３】

また、図22(3)に示すように、従来のIPv4及びIPv6処理においては、同図(1)及び(2)に示す如く、L2,L3,L4の処理順序又はこの逆でIP処理を行っており、この順序のカプセル化しか処理できず（プロトコル変換ができず）、別の順序の処理がある場合には予め用意しておかなければならないか、あるいは別のハードウェアを用意する必要が生じてしまう。

【００２４】

さらに、この例ではL3処理が2回行われるが、予めハードウェア的なプロトコルの処理順序を確定していないと設計ができなかったし、また考えられる限りのプロトコルの処理順序を組み込んでおくとしても、使わないプロトコルの処理順序をも設計しておかなければならないという問題があった。

【００２５】

従って本発明は、現存する多種多様なプロトコルに対して、それら一つ一つのパッケージを用意することなく、単体でプロトコル変換を実現することのできる通信装置を提供することを目的とする。

【発明の開示】

【００２６】

上記の目的を達成するため、本発明に係る通信装置は、受信パケットに含まれるプロトコル属性を検出し、該プロトコル属性に基づいてプロトコル処理順序を示すプロトコル処理順序データを生成するプロトコル処理順序データ生成部と、該プロトコル処理順序データに基づき該受信パケット中の複数のプロトコルを個別に処理するプロトコル変換部と、を備える。

【００２７】

すなわち、プロトコル処理順序データ生成部は、受信したパケットからプロトコル属性を検出する。このプロトコル属性は、例えば送信元のIPアドレス又は送信先のIPアドレスである。そして、プロトコル処理順序データ生成部は、そのプロトコル属性に基づいてプロトコル処理順序を示すプロトコル処理順序データを生成する。

【００２８】

プロトコル変換部は、プロトコル処理順序データ生成部から受けたプロトコル処理順序データに基づいて受信パケット中に設定されている複数のプロトコルの処理を行う。

【００２９】

このように、受信パケットに含まれるプロトコル属性がどのようなものであるかが判別できるので、このプロトコル属性に対応したプロトコルを用意しておけば、どのような受信パケットに対してもプロトコル処理順序データを生成することができ、このプロトコル処理順序データに基づいて受信したパケット中の複数のプロトコルを個別に処理することが可能となるので、単一の装置で複数のプロトコル変換を実現することができる。

【００３０】

従って、例えばIPv6のプロトコルで送信されたパケットを、IPv4のプロトコル上で送受信することができるなど、複数のプロトコル変換を必要とする通信装置を容易に実現することができる。

【００３１】

また上記のプロトコル処理順序データ生成部は、該プロトコル属性に対応したプロトコル総処理回数を該プロトコル処理順序データとして生成し、プロトコル変換部は、該プロトコル総処理回数分だけ該受信パケット中に設定された複数のプロトコルを先頭から順次処理することができる。

【００３２】

すなわち、プロトコル処理順序データ生成部は、該プロトコル属性に対応したプロトコル総処理回数を上記のプロトコル処理順序データとして生成し、このプロトコル総処理回

数に基づいてプロトコル変換部が受信パケット中に設定された複数のプロトコルを先頭から順次実行する。

【００３３】

従って、プロトコル属性が受信パケット中の複数のプロトコルを先頭から順次処理することを示している場合において、そのプロトコル属性に対応したプロトコル総処理回数分だけ受信パケット中のプロトコルを先頭から順次処理して行けば全てのプロトコルを正常に処理することが可能となる。

【００３４】

また本発明では、上記のプロトコル処理順序データ生成部は、該プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを先頭から順次該プロトコル処理部で処理させるヘッダ識別部と、該プロトコル処理部でのプロトコル処理回数をカウントするカウンタとを備え、該ヘッダ識別部は、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了する。

【００３５】

すなわち、この場合には、プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを受信パケットに付加してプロトコル変換部に送る。プロトコル変換部は、ヘッダ識別部でそのヘッダを識別して受信パケット中のプロトコルを先頭から順次プロトコル処理部で処理させ、このときのプロトコル処理回数をカウンタがカウントする。

【００３６】

そして、ヘッダ識別部は、カウンタによるプロトコル処理回数が上記のプロトコル総処理回数に達したときにプロトコル処理を終了するようにしている。

【００３７】

また本発明では、該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを先頭から順次該プロトコル処理部で処理させるヘッダ処理部と、該ヘッダ識別部でのプロトコル処理結果を識別し、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了させる処理完了部とを備えることができる。

【００３８】

この場合には、上記と同様にプロトコル総処理回数を含んだヘッダを受信パケットに付加してプロトコル変換部に与えるが、このプロトコル変換部では、ヘッダ処理部が上記のヘッダを識別して受信パケット中のプロトコルを先頭から順次プロトコル処理部で処理させるときのプロトコル処理回数を処理完了部で蓄積し、プロトコル処理回数が上記のプロトコル総処理回数に達したときに処理完了部がプロトコル処理を終了させる点が異なっている。

【００３９】

また、本発明では、該プロトコル処理順序データがプロトコル総処理回数を含んでおり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該受信パケットを待機させるデータ待機部と、該プロトコル処理順序データに基づいて該データ待機部における該受信パケット中のプロトコルを該プロトコル処理部で先頭から順次処理させると共に、該プロトコル処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が該プロトコル総処理回数に達したときプロトコル処理を終了させる処理順序制御部とを備えることができる。

【００４０】

すなわち、この場合には、プロトコル変換部において、プロトコル処理順序データとしてのプロトコル総処理回数に基づいてデータ待機部で待機させた受信パケット中のプロトコルを、処理順序制御部がプロトコル処理部で先頭から順次処理させる。

【００４１】
そして、処理順序制御部は、プロトコル処理部でのプロトコル処理回数を蓄積し、このプロトコル処理回数が上記のプロトコル総処理回数に達したときプロトコル処理を終了させるようにしている。
【００４２】
また本発明では、該プロトコル属性が、該複数のプロトコルを先頭から順次処理するのではなく、該プロトコル属性に対応した所定の処理順序を必要としていることを示しているとき、該プロトコル処理順序データ生成部は、該プロトコル総処理回数に該所定の処理順序を付加した該プロトコル処理順序データを生成し、該プロトコル変換部は、該所定の処理順序に従って該複数のプロトコルを該プロトコル総処理回数分だけ処理することができる。
【００４３】
すなわち、この場合には、プロトコル属性が上記とは異なり、複数のプロトコルを先頭から順次処理するのではなく、プロトコル属性に対応した所定の処理順序を必要としていることを示している場合、プロトコル総処理回数だけではプロトコル処理順序データとして不足している。
【００４４】
そこで、プロトコル処理順序データ生成部では、プロトコル総処理回数に、上記の所定の処理順序を付加したプロトコル処理順序データを生成する。この所定の処理順序に従ってプロトコル変換部は受信パケット中の複数のプロトコルをそのプロトコル総処理回数分だけ実行する。
【００４５】
これにより、受信したパケットに含まれる複数のプロトコルが先頭から順次処理するようなものではない場合でも、そのプロトコル属性に対応した所定の処理順序を予め用意しておけば、その所定の処理順序に従ってプロトコル総処理回数分だけ実行することでプロトコル変換を実現することが可能となる。
【００４６】
また本発明では、該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させるヘッダ識別部と、該プロトコル処理部でのプロトコル処理回数をカウントするカウンタとを備え、該ヘッダ識別部は、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了することができる。
【００４７】
すなわち、この場合には、上記において、プロトコル総処理回数だけでなくプロトコル属性に対応した所定の処理順序を含んだヘッダを受信パケットに付加する。プロトコル変換部では、上記のように受信パケット中のプロトコルを先頭から順次処理するのではなく、上記の所定の処理順序に従ってプロトコル処理部で処理させる。
【００４８】
そして、このプロトコル処理部でのプロトコル処理回数をカウンタでカウントし、カウントしたプロトコル処理回数と上記のプロトコル総処理回数とを比較し、両者が一致したときにヘッダ識別部がプロトコル処理を終了するようにしている。
【００４９】
また、本発明では、該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させるヘッダ処理部

と、該ヘッダ処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了させる処理完了部とを備えることができる。

【００５０】

すなわち、この場合には、プロトコル属性に対応した所定の実行順序を必要としていることを前提して、この所定の処理順序とプロトコル総処理回数とを含んだヘッダを受信パケットに付加してプロトコル変換部に送る。

【００５１】

プロトコル変換部では、ヘッダ処理部が受信パケット中のプロトコルを所定の処理順序で個々のプロトコル処理部により実行させ、このときのプロトコル処理回数を処理完了部が蓄積し、且つプロトコル処理回数が上記のプロトコル総処理回数に達したとき処理完了部がプロトコル処理を終了させるようにしている。

【００５２】

また、本発明では、該プロトコル処理順序データが該プロトコル処理回数及び該プロトコル属性に対応した所定の処理順序を含んでおり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該受信パケットを待機させるデータ待機部と、該プロトコル処理順序データに基づいて該データ待機部における受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させると共に、該プロトコル処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が該プロトコル総処理回数に達したときプロトコル処理を終了させる処理順序制御部とを備えていることができる。

【００５３】

すなわち、この場合には、やはりプロトコル属性に対応した所定の処理順序を必要としていることを前提として、プロトコル変換部では、そのプロトコル処理順序データに基づいてデータ待機部に待機させていた受信パケット中のプロトコルを、該処理順序制御部が該所定の処理順序でプロトコル処理部に実行させる。

【００５４】

そして、処理順序制御部は、プロトコル処理部でのプロトコル処理回数を蓄積し、このプロトコル処理回数が上記のプロトコル総処理回数に達したとき該プロトコル処理を終了させるようにしている。

【００５５】

なお、上記のプロトコル属性がセキュリティ・ゲートウェイを示しているとき、該所定の処理順序に暗号化処理を含ませることができる。

【００５６】

さらに、上記のヘッダ識別部は、対応するプロトコルを識別して対応する個々のプロトコル処理部に処理させることができる。

【００５７】

また、上記のヘッダ処理部は、各プロトコル処理部毎にヘッダ識別部を有し、各ヘッダ識別部が、対応するプロトコルを識別して対応するプロトコル処理部に処理させることができる。

【００５８】

さらに、上記のプロトコル処理順序データ生成部は、該プロトコル属性と該プロトコル処理順序データとを対応させたテーブルを備えることができる。

【００５９】

さらに、上記のプロトコル変換部は、プロトコル処理後は該プロトコル処理順序データを除去する除去部を有することができる。

【発明を実施するための最良の形態】

【００６０】

実施例(1)

図1は、図18に示したLNS12や、図19に示したセキュリティ・ゲートウェイSG2などに適

用される本発明に係る通信装置の実施例(1)を示したものである。この通信装置は、インターネット網などからの受信パケットをラッチするFiFo21と、このFiFo21から出力された受信パケットにヘッダを付加するヘッダ付加部22と、このヘッダ付加部22から出力されたヘッダ付の受信パケットを入力してそのヘッダを識別するヘッダ識別部23と、このヘッダ識別部23で識別されたプロトコルに対応する個別プロトコル処理部24a～24xを有するプロトコル処理部24と、このプロトコル処理部24でプロトコル処理されたときの処理回数をカウントする処理回数カウンタ25と、このカウンタ25が処理回数をヘッダ識別部23に与えた結果、ヘッダ識別部23が受信パケットの処理を完了したと判定したことを知らされる処理完了部26と、処理完了時に受信パケットからヘッダを除去するヘッダ除去部27とを備え、処理完了部26からはデータ送出許可信号DTEがFiFo21に与えられるようになっている。

【００６１】

図2は、図1に示したヘッダ付加部22の実施例(1)を示したものである。
このヘッダ付加部22は、FiFo21からのパケットP2（図18,19のパケットP2参照）を格納するバッファ31と、このバッファ31に格納されたパケットP2における送信元IPアドレスを抽出する送信元IPアドレス抽出部32と、送信元IPアドレス抽出部32で抽出された送信元IPアドレスを元に処理順序ヘッダ情報を出力するプロトコル属性テーブル33と、テーブル33からの処理順序ヘッダ情報に基づいてヘッダを作成するヘッダ作成部34、バッファ31からパケットP2を入力してヘッダ作成部34からのヘッダを組み込むヘッダ組込部35とで構成されている。

【００６２】

図2に示したプロトコル属性テーブル34の一実施例が図3に示されている。図示のように、このテーブルは、送信元IPアドレス（32ビット）とプロトコル属性と処理順序ヘッダ情報とで構成されており、送信元IPアドレスから、処理順序ヘッダ情報としてのプロトコル処理回数とプロトコル総処理回数とプロトコルの処理順序とが読み出されるようになっている。

【００６３】

なお、送信元IPアドレスの代わりに送信先IPアドレスを用いても同様のテーブルとなる。

【００６４】

図4は、図1に示したヘッダ識別部23の一実施例を示している。この実施例では、ヘッダ付加部22からのヘッダが付加された受信パケットがバッファ41に格納され、その中のヘッダのみがデコーダ42に与えられるようになっている。デコーダ42はN個のセレクタ43_1～44_Nで構成されたセレクタ部43に接続されており、これらN個のセレクタ43_1～43_Nは同じN個のバッファ44_1～44_Nで構成されたバッファ部44に個々に接続されている。

【００６５】

そしてこれらのバッファ44_1～44_Nはそれぞれプロトコル処理部24を構成する個別プロトコル処理部24a～24x（図1参照）に接続されており、バッファ部44の各出力はN：1セレクタ45に接続され、その内の一つの出力がデコーダ42の制御により、選択されて処理回数カウンタ25をカウントアップし、その結果（ヘッダ）がバッファ41に戻されるようになっている。

【００６６】

また、受信パケットはバッファ41から、デコーダ42の制御を受けるセレクタ46を経由してバッファ47に送られ、このバッファ47から処理完了部26を経由してヘッダ除去部27に送られるようになっている。

【００６７】

図5は、図2に示したヘッダ作成部36で作成されるヘッダの一実施例を示したものであり、図3に示した属性テーブルにおける「プロトコル現処理回数」と「プロトコル総処理回数」とN個の「処理プロトコル番号」が直列配置されて可変長ヘッダを構成している。

【００６８】

図6は、図18に示したようなLNSに図1の実施例を組み込んだ場合のプロトコル変換処理

をシーケンスで示したものである。以下、この図6を参照して図1から図5に示した実施例(1)の動作を説明する。

【００６９】

まず、インターネット網等から図6(1)に示すパケットをFiFo21で受信し、さらにこの受信パケットをヘッダ付加部22に送る。ヘッダ付加部22では、図2に示すように、バッファ31を経由して送信元IPアドレス抽出部32で受信パケットの送信元IPアドレスを抽出する。

【００７０】

今、この受信パケットの送信元IPアドレスが図3に示すように「255.255.255.0」である場合、この属性テーブル33に示すようにプロトコル属性はLNS(L2TP)であることが分かる。

【００７１】

従って、この送信元IPアドレスに基づいて属性テーブル33からはプロトコル総処理回数“５”と現在のプロトコル処理回数“０”から成るヘッダがヘッダ作成部34で作成され、ヘッダ組込部35で受信パケットに組み込まれて、図6(2)に示すようなヘッダが付加された受信パケットとなる。

【００７２】

この受信パケットのペイロードには、図示の如く、IP(x→y),UDP,L2TP,PPP,IP(a→b)の各プロトコルが付加設定されている。これは図3に示すプロトコル属性がLNSの場合において、処理順序ヘッダ情報として示される“１”（IPv4処理）,“６”（UDP処理）,“７”（L2TP処理）,“３”（PPP処理）,“１”（IPv4処理）に対応している。

【００７３】

但し、この実施例ではこの受信パケットにはプロトコル総処理回数とプロトコル現処理回数が付加されるだけである。従って、この場合には、図5に示したヘッダでは第1～N処理プロトコル番号は不用となる。

【００７４】

このようにしてヘッダが付加された受信パケットは、ヘッダ識別部23に送られる。ヘッダ識別部23では、まずバッファ41に格納された後、その内のヘッダのみが図6(5)に示すように取り出されてデコーダ42に与えられる。

【００７５】

デコーダ42は、セレクタ部43及び46を制御するようにこれらと接続されており、入力したヘッダに基づき、最初はプロトコル総処理回数が“５”であり、現在のプロトコル処理回数“０”とは一致しないので、プロトコル処理を実行する必要があり、このためセレクタ部43を制御してバッファ41の受信パケットをバッファ部44に転送する。

【００７６】

すなわち、デコーダ42はプロトコル総処理回数のみを見ているので、例えばセレクタ部43を図4における上から順々に指定して行くことが可能である。従って、まずセレクタ部43の一番上側のセレクタ43_1が指定されたとすると、バッファ41からの受信パケットはセレクタ43_1を経由してバッファ部44のバッファ44_1に格納される。

【００７７】

バッファ44_1に格納された受信パケットは、図1に示すプロトコル処理部24における個別プロトコル処理部24a～24xのいずれかにより処理される。例えば、バッファ44_1には個別プロトコル処理部24aが対応しているとすると、受信パケットはこの個別プロトコル処理部24ａによってプロトコル処理が実行される。

【００７８】

図6に示したLNS処理の例では、まずIP終端処理が実行されることとなり（同図(3)）、終端後は、同図(4)に示すように一つのプロトコル、すなわちIP(x→y)プロトコル処理が完了したことになる。

【００７９】

このIP処理後の受信パケットはバッファ44_1から、やはりデコーダ42の制御下にあるセレクタ45を経由して処理回数カウンタ25に与えられ、カウンタ25の値が“１”だけインク

リメントされて、バッファ41に戻される。

【００８０】

この結果、同図(5)に示すようにプロトコル総処理回数が“５”で、現在のプロトコル処理回数が“１”となったヘッダがバッファ41において受信パケットに付加される。

【００８１】

この後、デコーダ42は次にセレクタ43_2を指定し、このセレクタ43_2を経由してバッファ41の受信パケットがバッファ44_2に送られ、同図(6)の状態から同図(7)に示すようにUDPプロトコル処理部24bによる終端処理が行われて、同図(8)に示すようなUDPプロトコルが取り除かれた受信パケットとなる。

【００８２】

そして、この結果、やはり処理回数カウンタ25が“１”だけインクリメントされてバッファ41にヘッダ（同図(8)参照）として戻されるので、デコーダ42のヘッダは同図(9)に示すようにプロトコル処理回数が“２”に更新される。

【００８３】

以下同様にして、LNS処理における「L2TP処理」と「PPP処理」と「IP(a→b)処理」とが同図(10)～(20)に示すとおり実行される。そして、同図(20)に示すようにプロトコル総実行回数と現在のプロトコル処理回数とが共に“５”となって等しくなった時、プロトコル処理は完了したことを示している。

【００８４】

そこで、デコーダ42は今度は、セレクタ46を制御することによりバッファ41の受信パケットをバッファ47に送り、そこからさらに処理完了部26に送る。処理完了部26は次のデータ送出許可信号DTEをFiFo21に送ると共に、同図(20)に示したパケットをヘッダ除去部27に送ると、ヘッダ除去部27では、同図(21)に示すようなヘッダ除去後のパケットを出力することになる。

【００８５】

なお、この実施例では、データ送出許可信号DTEをFiFo21に送って次の受信パケットの取込を行っているが、これに限らず、ヘッダ識別部23自身でパケットの取込を逐次行ってもよい。

【００８６】

図7に示すシーケンス図は、図6に示したLNS処理ではなく、図18に示したようなLACに図1の実施例を組み込んだ場合のプロトコル総処理回数制御を示したものである。

【００８７】

この図7の処理例と図6の処理例は、図3の属性テーブルから分かるように、LAC処理の場合にはプロトコル総処理回数が“４”であり、LNSより“１”だけ少ないことが異なっている。従って、ヘッダの生成においては、図7(2)に示すように総実行回数を“４”として現在のプロトコル処理回数が“４”になるまで実行すると、処理後のパケットは同図(19)に示すようになる。すなわち、最後のIP(a→b)のプロトコル処理が実行されないことになる。

【００８８】

その他の処理は、図6と同様である。

【００８９】

この実施例(1)において、図6及び図7に例示したように受信パケットに付加するヘッダがプロトコル総処理回数と現在のプロトコル処理回数のみから成る場合は、前述の如くプロトコル処理を受信パケットの先頭から順次実行すれば良いことを前提にしている。

【００９０】

しかしながら、図8及び図9に示すように単にプロトコル総処理回数分だけ実行したのでは処理ができない場合が存在する。

【００９１】

まず、図8の例においては、同図(1)の受信パケットに対してヘッダ（図示せず）を同図(2)に示すように生成したとすると、同図(3)に示すIP(x→y)の終端処理プロトコルを実行

した後、同図(4)のパケットを同図(5)に示す状態からUDP終端処理を行おうとした場合、ペイロードが暗号化されているためこのUDP終端処理が行えないことになる。

【００９２】

また、図9の例に示すように、同図(1)の受信パケットに対して同図(2)のヘッダを生成し、これに対して同図(3)において暗号解読処理を実行しようとすると、今度はペイロードが暗号化されていないため暗号解読処理後のパケットは処理できないことになる。

【００９３】

そこで、上記のようにプロトコル総処理回数だけではなく、暗号化処理などを考慮して所定の順序で処理を行う場合の順序処理データをヘッダに付加する必要がある。この場合の実施例が図10に示されている。なお、この図10の動作実施例の場合も上記の図1～図5に示した構成は同様に適用できる。

【００９４】

まず、図10(1)に示す受信パケットに対して、ヘッダ付加部22では同図(2)に示すようにプロトコル総処理回数及びプロトコル処理回数に加えて、ペイロードが暗号化されていることに伴い、まず暗号化処理（図21(10)～(12)参照）のプロトコルを加えるとともにIP(x→y)の処理プロトコルを加えたヘッダをヘッダ識別部23に与える。

【００９５】

ヘッダ識別部23では、ヘッダを識別してまず暗号解読処理を行うため、受信パケットを図1に示した例えばプロトコル処理部24xに与えることにより同図(3)に示す受信パケットから同図(4)に示す暗号解読処理後のパケットが得られる。

【００９６】

このときのヘッダは、同図(5)に示すようにプロトコル処理回数が“１”にインクリメントされた形になる。

【００９７】

同図(6)に示すようにヘッダと受信パケットとがバッファ41で組み合わされて、さらに同図(6)に示すように次の処理へ進むと、今度はプロトコル処理部24の図示しない別の個別プロトコル処理部において、同図(7)に示す受信パケットがIP(x→y)の終端処理を受けることにより同図(8)に示す受信パケットにデカプセル化される。

【００９８】

このときヘッダは、同図(9)に示すようにプロトコル処理回数が“２”となり、プロトコル総処理回数“２”と一致するので、ヘッダと受信パケットが合わされたパケットは処理完了部26において処理終了とされ、さらにヘッダ除去部27でヘッダが除去されて、同図(11)に示す処理後のパケットが得られることになる。

【００９９】

図11(1)は、IPv4とIPv6のトンネル接続におけるヘッダ付加部の実施例を示したものである。すなわち、この実施例の場合には図2に示したような属性テーブルは必要なく、その代わりに、バッファ31で受信した受信パケットにおけるバージョン情報を確認して処理ヘッダ情報を作成する処理ヘッダ情報作成部36をヘッダ作成部34の前に設けた点が異なっている。

【０１００】

すなわち、図11(2)に示すようにIPv4とIPv6のトンネルは4つのパターンしかないので、処理順序ヘッダ情報作成部36に予めこのバージョン情報を与えておけば、ヘッダ作成部34は属性テーブルがなくてもヘッダを作成することができる。（但し、このようなIPv4/v6処理専用のパケットにのみ適用されることは言うまでもない。）

このときのアルゴリズムを示したのが図12である。すなわち、例えば図11(2)の一番上の例の場合では、まずMACヘッダの識別を行い(ステップS1)、IPヘッダの識別、バージョン(v4/v6)の確認、ヘッダ長の確認、パケット長の確認、ヘッダチェックサムなどを実行し(ステップS2)、ヘッダがOKかどうかを判定する（ステップS3）。

【０１０１】

ステップS2の実行により、ヘッダがOKであれば、IPv4か否かを判定し（ステップS4）、

IPv4のときには、プロトコル総処理回数を“１”だけインクリメントして処理プロトコルをIPv4とし、IPv4でない場合には、プロトコル総処理回数を“１”だけインクリメントすると共に処理プロトコルをIPv6に設定する。

【０１０２】

ヘッダがOKでないとき、すなわちヘッダが全てチェックが終わってペイロードが検出されたときにはヘッダ作成部34に対して、プロトコルの種類とその現処理回数及び総処理回数を与える。このようにしてプロトコル総処理回数と現処理回数と実行すべき処理プロトコルをヘッダに組み込むことが可能となる。

【０１０３】

実施例(2)

図13は、本発明に係る通信装置の実施例(2)を示したものである。図1の実施例(1)では、プロトコル処理部24が個別プロトコル処理部24a～24xを並列した形で備えており、ヘッダ処理部23でのヘッダ識別により、対応する個別プロトコル処理部24a～24xを選択してプロトコル処理を実行しているが、図13の実施例(2)の場合には、ヘッダ識別部74a～74xを直列接続したヘッダ処理部74を設け、各ヘッダ識別部74a～74xに対して、プロトコル処理部75を構成する個別プロトコル処理部75a～75xを個々に相互接続させている点が主に異なった点である。

【０１０４】

具体的には、受信パケットにヘッダを付加するヘッダ付加部71と、このヘッダ付加部71からFiFo73への入力を制御するFiFo入力制御部72と、FiFo73から出力された受信パケットをヘッダ処理部74を経由して入力しパケットが処理完了しているか否かを識別する処理完了部76と、この処理完了部76で完了識別された受信パケットのヘッダを除去するヘッダ除去部77とを備え、処理完了部76からFiFo入力制御部72へ処理経過の信号が与えられている。

【０１０５】

図14には、図13に示した各ヘッダ識別部74a～74xの具体的な実施例が示されている。すなわち、受信パケットはまずバッファ41に入力され、その内のヘッダがデコーダ42に与えられる点は図4の実施例と同様である。また、この場合、2つセレクタ43と46のみが設けてあり、それぞれデコーダ42から制御を受けるようになっており且つバッファ41から受信パケットを入力するようになっている。

【０１０６】

そして、自分がヘッダ識別を行う場合には、デコーダ42からセレクタ43が選択されるため、バッファ41の受信パケットはセレクタ43を介してバッファ44に送られる。そしてこのバッファ44はプロトコル処理部75における図示しない対応した個別プロトコル処理部に送られてプロトコル処理を行った後、再びバッファ44に戻され、さらにセレクタ48に送られる。

【０１０７】

セレクタ48はデコーダ42から同様に制御を受け、この場合にはバッファ44とセレクタ46のうち、自分がヘッダ識別を行ったのであるからバッファ44が選択され、受信パケットは次段のヘッダ識別部のバッファ41に送られることとなる。

【０１０８】

これを繰り返して行くことにより、全てのヘッダ識別を行い且つそれに対応した個別のプロトコル処理が実行されることとなる。

【０１０９】

通常は、ヘッダ処理部74は必要なヘッダ識別部を有し、各ヘッダ識別部は対応する個別プロトコル処理部に接続されているので、このヘッダ処理部74を通過した受信パケットは処理完了部76で処理完了したことが判明することとなり、その場合には次のパケットがFiFo73に入力されるようにFiFo入力制御部72で制御する。

【０１１０】

これと共に、処理完了した受信パケットはヘッダ除去部77でヘッダが除去されて出力さ

れることとなる。

【０１１１】

なお、この場合も、処理完了部76からFiFo入力制御部72へ次のパケットを入力するための信号を与えなくてもヘッダ処理部74は順次プロトコル処理を実行してもよい。

【０１１２】

上記のような動作は、図6及び図7に示したプロトコル総処理回数に基づくプロトコル変換だけでなく、図10に示したプロトコル総処理回数並びにプロトコル属性に対応した所定の処理順序をヘッダに付加して行う場合も同様に適用できる。

【０１１３】

すなわち、図6の例では、ヘッダ付加部71において同図(2)に示すようなヘッダが付加された受信パケットがFiFo入力制御部72及びFiFo73を経由してヘッダ処理部74に送られる。

【０１１４】

ヘッダ処理部74では、ヘッダ識別部74a～74xがそれぞれ、IP(x→y),UDP,L2TP,PPP,IP(a→b)のプロトコル処理を行うように順次並べられているとすると、これに対してプロトコル処理部75における個別プロトコル処理部75a～75xも対応したプロトコル処理プログラムが格納されていることとなり、同図(3)以降に示す手順を、ヘッダ識別部74a→74xにおいて順次実行して行けばよい。

【０１１５】

そして、このヘッダ処理部74を通過した後は処理完了部76で処理完了が検出され、ヘッダ除去部77でヘッダが除去されたものが図6(21)に示す処理後のパケットとなる。

【０１１６】

これは、図7の例も同様である。

【０１１７】

さらに、このような処理は、図10に示した所定の処理順序をヘッダに加えた場合も同様である。

【０１１８】

すなわち、同図(2)に示すようにヘッダにプロトコル総処理回数だけでなく、このときのプロトコル属性に対応した暗号処理及びIP処理をヘッダに付加した受信パケットがヘッダ付加部71からFiFo入力制御部72及びFiFo73を経由してヘッダ処理部74に送られる。

【０１１９】

このヘッダ処理部74における各ヘッダ識別部74a～74xは、暗号化処理のプロトコル又はIP処理のプロトコルであるか否かを識別し、例えばヘッダ識別部74xがそのプロトコルをデコーダ42で例えば暗号処理であると識別した場合には、対応する個別プロトコル処理部75xにその受信パケットを処理させ、その処理した受信パケットを入力してさらに次のヘッダ識別部に渡す。

【０１２０】

これを順に繰り返すことにより、処理完了部76では図10(11)に示す受信パケットが得られ、これをヘッダ除去部77でヘッダを除去することにより処理後のパケットが得られることになる。

【０１２１】

実施例(3)

図15は本発明に係る通信装置の実施例(3)を示したものである。上記の実施例(1)及び(2)では、ヘッダ付加部を用いてプロトコル処理順序データとしてのヘッダを生成し且つ受信パケットに付加しているが、この実施例(3)では受信パケットにヘッダという形で付加するのではなく、プロトコル処理順序データとして処理順序データ生成部92がこれを別個に生成し、且つ処理順序制御部93に処理順序データPDとして与える。

【０１２２】

また処理順序データ生成部92からはパケットがデータ待機部94に与えられ、処理順序制御部93はプロトコル指示信号DSをデータ待機部94に与えることにより、データ待機部94は対応するプロトコル処理部95の個別プロトコル処理部95a～95xに受信パケットを送って処

理を行わせる。

【０１２３】

その実行の終了信号FSをプロトコル処理部95が処理順序制御部93に送ると共に、処理し終わった受信パケットはデータ待機部94に保持しておく。

【０１２４】

さらに次の処理プロトコルによってプロトコル処理部95に処理を行わせるようにし、最終的に処理が終わった段階でデータ待機部94から処理完了部96を経由して処理パケットを得ようとするものである。

【０１２５】

この場合の主にデータ待機部94の構成例を示したものが図16に示されている。

【０１２６】

すなわち、FiFo91より処理順序データ生成部92を経由して送られて来たパケットはバッファ94_0に格納される。

【０１２７】

一方、処理順序データ生成部92は、処理順序制御部93からの処理順序データ要求DRを受けて処理順序データPDを与えるようになっており、処理順序制御部93はセレクタ94_1～94_yを制御してバッファ94_0に格納されている受信パケットを対応する個別プロトコル処理部95a～95xに与えて処理を行わせ、この処理結果を同じセレクタを経由してバッファ94_0に戻すようにしている。

【０１２８】

このような制御を繰り返すことにより、処理順序データPDに基づいて処理が終了した（プロトコル現処理回数＝プロトコル総処理回数）と判断した処理順序制御部93はセレクタ94_yを経由してバッファ94_0から、処理が完了したパケットを処理完了部96に与え、完了処理されたパケットを出力するようにしている。

【０１２９】

図17(1)には、図16に示した処理順序制御部93の処理アルゴリズムが示されており、これはセレクタ94_1～94_x及び94_yをどのように制御するかを示したものである。

【０１３０】

すなわち、図17(2)に例示した処理順序データPDを処理順序データ生成部92から入力すると（ステップS11）、プロトコル処理回数をi、プロトコル総処理回数をNとして（ステップS12）、プロトコル(i)の処理を対応するセレクタ94_1～94_x(x≧N)に指示する（ステップS13）。

【０１３１】

そして、プロトコル(i)が終了したか否かを判定し、終了していないときはステップS13に戻るが、プロトコル(i)が終了したときにはi=Nであるか否かを判定し、両者が不一致の場合にはiを“１”だけインクリメントしてステップS13に戻るが、i=Nであることが分かったときには処理完了として、セレクタ94_yを制御することによりバッファ94_0から受信パケットを処理完了部96に与えることができる。

【０１３２】

このように実施例(3)においても、図17(2)に示すように処理順序データPDはプロトコル処理回数とプロトコル総処理回数並びに必要に応じて所定の順序に従ったプロトコルが格納されているので、上記の実施例(1)及び(2)でそれぞれ説明したのと同様のプロトコル処理を実行することができる。

【０１３３】

すなわち、例えば図6のLNS処理の場合には図17(2)に示す処理順序データPDはプロトコル処理回数とプロトコル総処理回数しか含まれていないが、プロトコル処理部95における個別プロトコル処理部95a～95xに対応したセレクタ94_1～94_xにプロトコル実行指示DSを順次与えれば、図6(3)から同図(20)に示すプロトコル処理を順次実行することができる。

【０１３４】

この処理の終了によりセレクタ94_yを介して最終的なパケットを94_0からヘッダ除去さ

れた形で処理完了部96から得られることになる。

【０１３５】

また、図10に示す所定の処理順序データを用いる場合は、図17(2)に示す処理順序データPDそのものであるので、これが適用できることは言うまでもない。

【０１３６】

以上説明したように本発明に係る通信装置によれば、受信パケットに含まれヘッダ識別部74a～74xを直列接続したるプロトコルの属性を検出し、該プロトコル属性に基づいてプロトコル処理順序を示すプロトコル処理順序データを生成するプロトコル処理順序データ生成部と、該プロトコル処理順序データに基づき該受信パケット中の複数のプロトコルを処理するプロトコル変換部とを備えたので、例えば図20に示したような例において、従来であればセキュリティ・ゲートウェイSG2にLNSも配備し、いずれのモードまたはセッションにも対応できるようにしなければならないが、一つの装置においてあらゆるプロトコルに対応することができ、考えられる全てのパケットの受信に一つの装置で対応することが可能となる。

（付記）

１．受信パケットに含まれるプロトコル属性を検出し、該プロトコル属性に基づいてプロトコル処理順序を示すプロトコル処理順序データを生成するプロトコル処理順序データ生成部と、

該プロトコル処理順序データに基づき該受信パケット中の複数のプロトコルを個別に処理するプロトコル変換部と、

を備えたことを特徴とする通信装置。

２．付記１において、

該プロトコル処理順序データ生成部は、該プロトコル属性に対応したプロトコル総処理回数を該プロトコル処理順序データとして生成し、プロトコル変換部は、該プロトコル総処理回数分だけ該受信パケット中に設定された複数のプロトコルを先頭から順次処理することを特徴とした通信装置。

３．付記１において、

該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを先頭から順次該プロトコル処理部で処理させるヘッダ識別部と、該プロトコル処理部でのプロトコル処理回数をカウントするカウンタとを備え、該ヘッダ識別部は、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了することを特徴とした通信装置。

４．付記１において、

該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを先頭から順次該プロトコル処理部で処理させるヘッダ処理部と、該ヘッダ識別部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了させる処理完了部とを備えていることを特徴とした通信装置。

５．付記１において、

該プロトコル処理順序データがプロトコル総処理回数を含んでおり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該受信パケットを待機させるデータ待機部と、該プロトコル処理順序データに基づいて該データ待機部における受信パケット中のプロトコルを該プロトコル処理部で先頭から順次処理させると共に、該プロトコル処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が該プロトコル総処理回数に達したときプロトコル処理を終了させる処理順序制御部とを備えていることを特徴とした通信装置。

６．付記２から５のいずれか一つにおいて、
該プロトコル属性が、該複数のプロトコルを先頭から順次処理するのではなく、該プロトコル属性に対応した所定の処理順序を必要としていることを示しているとき、該プロトコル処理順序データ生成部は、該プロトコル総処理回数に該所定の処理順序を付加した該プロトコル処理順序データを生成し、該プロトコル変換部は、該所定の処理順序に従って該複数のプロトコルを該プロトコル総処理回数分だけ処理することを特徴とした通信装置。
７．付記１において、
該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させるヘッダ識別部と、該プロトコル処理部でのプロトコル処理回数をカウントするカウンタとを備え、該ヘッダ識別部は、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了することを特徴とした通信装置。
８．付記１において、
該プロトコル処理順序データ生成部が、該プロトコル処理順序データとしてプロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んだヘッダを該受信パケットに付加するヘッダ付加部であり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該ヘッダを識別して該受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させるヘッダ処理部と、該ヘッダ処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が、該プロトコル総処理回数に達したときプロトコル処理を終了させる処理完了部とを備えていることを特徴とした通信装置。
９．付記１において、
該プロトコル処理順序データが該プロトコル総処理回数及び該プロトコル属性に対応した所定の処理順序を含んでおり、該プロトコル変換部が、該複数のプロトコルを個別に処理するプロトコル処理部と、該受信パケットを待機させるデータ待機部と、該プロトコル処理順序データに基づいて該データ待機部における受信パケット中のプロトコルを該所定の処理順序で該プロトコル処理部により処理させると共に、該プロトコル処理部でのプロトコル処理回数を蓄積し、該プロトコル処理回数が該プロトコル総処理回数に達したときプロトコル処理を終了させる処理順序制御部とを備えていることを特徴とした通信装置。
１０．付記６から９のいずれか一つにおいて、
該プロトコル属性がセキュリティ・ゲートウェイを示しているとき、該所定の処理順序に暗号化処理を含むことを特徴とした通信装置。
１１．付記３又は７において、
該ヘッダ識別部が、対応するプロトコルを識別して対応する個々のプロトコル処理部に処理させることを特徴とした通信装置。
１２．付記４又は８において、
該ヘッダ処理部が、各プロトコル毎にヘッダ識別部を有し、各ヘッダ識別部が、対応するプロトコルを識別して対応するプロトコル処理部に処理させることを特徴とした通信装置。
１３．付記１から１２のいずれか一つにおいて、
該プロトコル属性が、送信元又は送信先のIPアドレスであることを特徴とした通信装置。
１４．付記１から１３のいずれか一つにおいて、
該プロトコル処理順序データ生成部が、該プロトコル属性と該プロトコル処理順序データとを対応させたテーブルを有していることを特徴とした通信装置。
１５．付記１から１４のいずれか一つにおいて、

該プロトコル変換部は、プロトコル処理後は該プロトコル処理順序データを除去する除去部を有することを特徴とした通信装置。

【図面の簡単な説明】

図１は、本発明に係る通信装置の実施例（１）を示したブロック図である。

図２は、本発明に係る通信装置に用いられるヘッダ付加部の実施例（１）を示したブロック図である。

図３は、図２に示したヘッダ付加部におけるプロトコル属性テーブルを示した図である。

図４は、本発明に係る通信装置の実施例（１）に用いられるヘッダ識別部の実施例を示したブロック図である。

図５は、本発明に係る通信装置に用いられるプロトコル処理順序データとして受信パケットに付加されるヘッダの実施例を示した図である。

図６は、本発明に係る通信装置の各実施例において、プロトコル処理回数制御のみを実行するＬＮＳの処理シーケンスを示した図である。

図７は、本発明に係る通信装置の各実施例において、プロトコル処理回数制御のみを実行するＬＡＣの処理シーケンスを示した図である。

図８は、図６及び図７に示すようなプロトコル総処理回数のみでプロトコル変換を行った場合の問題点を説明するためのシーケンス図（１）である。

図９は、図６及び図７に示すようなプロトコル総処理回数のみでプロトコル変換を行った場合の問題点を説明するためのシーケンス図（２）である。

図１０は、本発明に係る通信装置の各実施例において、上記のようにプロトコル総処理回数に加えて所定の処理順序をヘッダに付加した場合の実施例を示したシーケンス図である。

図１１は、本発明に係る通信装置の実施例に用いられるヘッダ付加部の実施例（２）を説明するためのブロック図である。

図１２は、図１１に示した処理順序ヘッダ情報作成部の動作フローチャート図である。

図１３は、本発明に係る通信装置の実施例（２）を示したブロック図である。　図１４は、図１３に示したヘッダ処理部における各ヘッダ識別部の実施例を示したブロック図である。

図１５は、本発明に係る通信装置の実施例（３）を示したブロック図である。

図１６は、図１５に示したデータ待機部を特に具体的に示したブロック図である。

図１７は、図１５及び１６に示した処理順序制御部の動作フローチャート図である。

図１８は、一般的に知られているインターネット網を経由したＰＰＰセッションとＬ２ＴＰセッションを示した通信システム図である。

図１９は、インターネット網を介してＩＰｓｅｃパケットを送る場合のトンネルモードとトランスポートモードを示した通信システム図である。

図２０は、図１９に加えて図１８に示したＰＰＰセッション及びＬ２ＴＰセッションを加えた場合の問題点を指摘するための図である。

図２１は、従来より知られているカプセル化したパケットの例を示した図である。

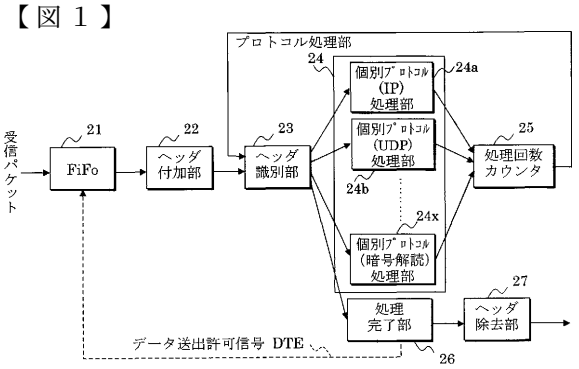
図２２は、ＩＰｖ４及びＩＰｖ６を処理する場合の従来から知られている方式を説明するためのブロック図である。

符号の説明

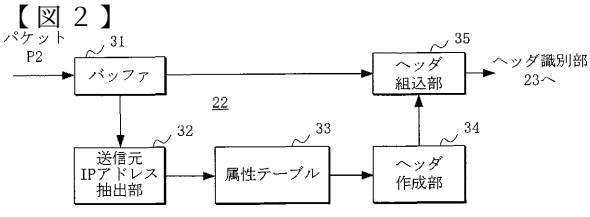
１０，１４，１５，１６，１７　ＰＣ
１１　ＬＡＣ（Ｌ２ＴＰ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）
１２　ＬＮＳ（Ｌ２ＴＰ　Ｎｅｔｗｏｒｋ　Ｓｅｒｖｅｒ）
１３，１３ａ，１３ｂ　ＬＡＮ
２１，７３，９１　ＦｉＦｏ
２２，７１　ヘッダ付加部
２３，７４ａ～７４ｘ　ヘッダ識別部
２４，７５，９５　プロトコル処理部
２４ａ～２４ｘ，７５ａ～７５ｘ，９５ａ～９５ｘ　個別プロトコル処理部

２５　処理回数カウンタ
２６，７６，９６　処理完了部
２７，７７　ヘッダ除去部
３１　バッファ
３２　送信元ＩＰアドレス抽出部
３３　属性テーブル
３４　ヘッダ作成部
３５　ヘッダ組込部
３６　処理順序ヘッダ情報作成部
７２　ＦｉＦｏ入力制御部
７４　ヘッダ処理部
９２　処理順序データ生成部
９３　処理順序制御部
９４　データ待機部
図中、同一符号は同一又は相当部分を示す。

【図１】



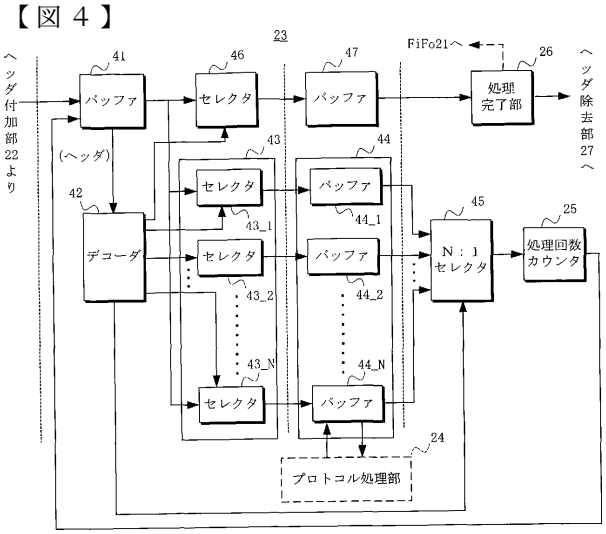
【図２】



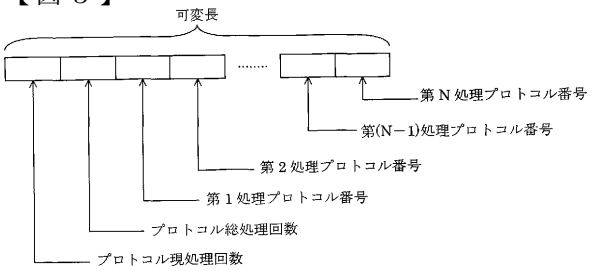
【図３】

送信元 IP アドレス (32 ビット)	プロトコル属性	処理順序ヘッダ情報 プロトコル現処理回数	プロトコル総処理回数	プロトコルの処理順序 (処理プロトコル)					備考
				1	6	7	3	1	
255.255.255.0	LNS(L2TP)	0	5						
12.3.4	LAC(L2TP)	0	4	1	6	7	3	0	
202.243.37.74	セキュリティ・ゲートウェイ (IP sec AH 認証)	0	2	4	1	0	0		
61.22.33.44	セキュリティ・ゲートウェイ (IP sec ESP 暗号)	0	3	5	1	1	0	0	トンネルモード
61.22.33.45	セキュリティ・ゲートウェイ (IP secESP 暗号)	0	2	5	1	0	0	0	トランスポートモード
125.30.33.2	ルータ (IPv6→IPv4 網のトンネル)	0	1	1	0	0	0	0	IPv6 パケットの IPv4 網へのトンネル化
5.5.5.5	ルータ (IPv4→IPv6 網のトンネル)	0	1	2	0	0	0	0	IPv4 パケットの IPv6 網へのトンネル化
125.30.33.20	ルータ (IPv6 網→IPv4 のトンネル)	0	2	2	1	0	0	0	IPv6 網からトンネル化された IPv4 の取出し
5.5.5.50	ルータ (IPv4 網→IPv6 のトンネル)	0	2	1	2	0	0	0	IPv4 網からトンネル化された IPv6 の取出し
125.30.33.20	ルータ (IPv4 網→IPv4 のトンネル)	0	2	1	1	0	0	0	IPv4 プローバル網からトンネル化された IPv4 (プライベート) の取出し
その他		0	0	0	0	0	0	0	
備考	処理プロトコル:1=IPv4 処理、2=IPv6 処理、3=PPP 処理、4=AH 認証処理、5=ESP 暗号解読、6=UDP 処理、7=L2TP 処理								

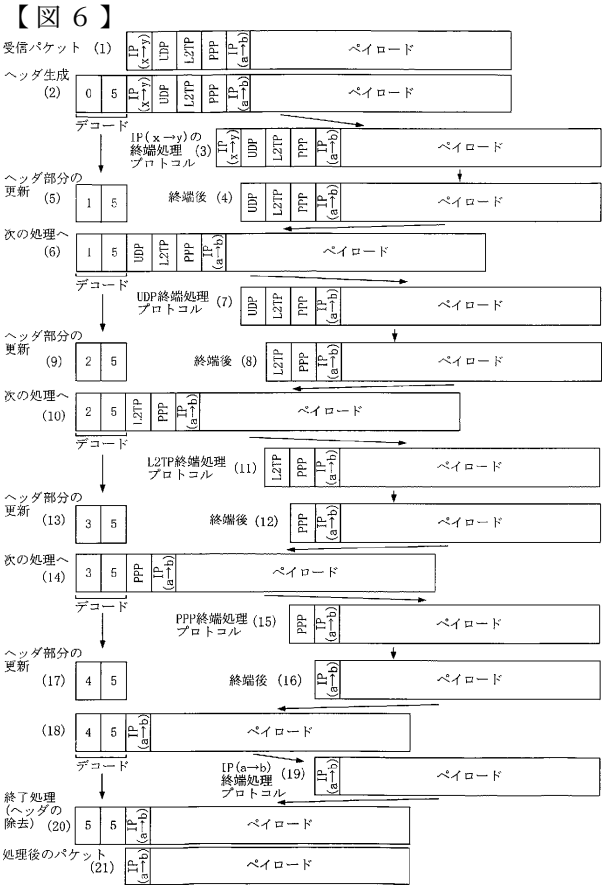
【図４】


23
FiFo21へ
ヘッダ付加部22より
ヘッダ除去部27へ
41
バッファ
46
セレクタ
47
バッファ
26
処理完了部
(ヘッダ)
42
デコーダ
43
セレクタ
43_1
セレクタ
43_2
セレクタ
43_N
セレクタ
44
バッファ
44_1
バッファ
44_2
バッファ
44_N
バッファ
45
N：1セレクタ
25
処理回数カウンタ
24
プロトコル処理部

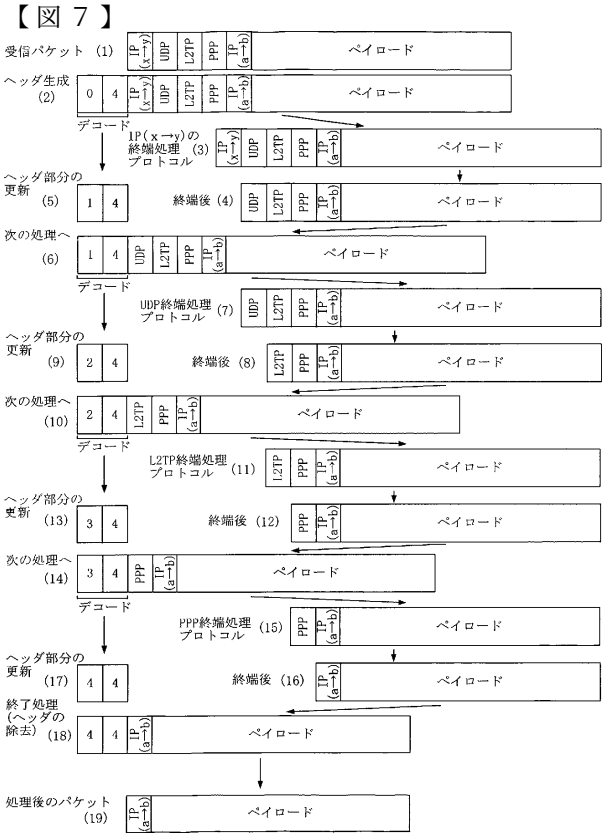
【図５】


可変長
第N処理プロトコル番号
第(N−1)処理プロトコル番号
第2処理プロトコル番号
第1処理プロトコル番号
プロトコル総処理回数
プロトコル現処理回数

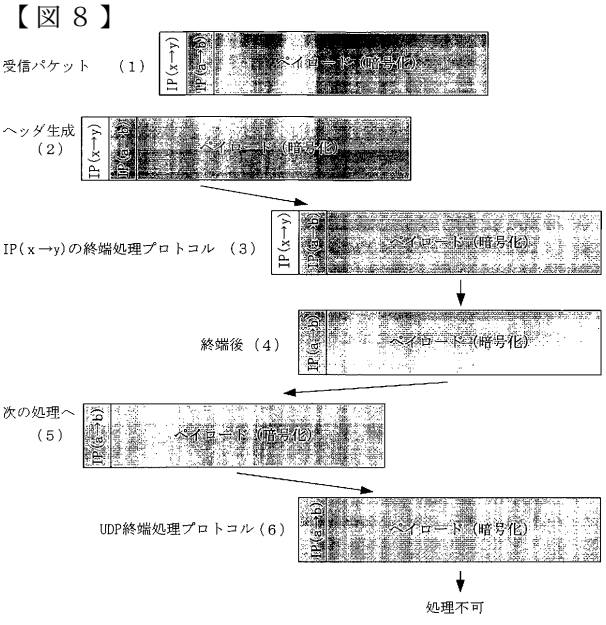
【図６】


受信パケット (1)
ヘッダ生成 (2)
デコード
IP(x→y)の終端処理 (3) プロトコル
ヘッダ部分の更新 (5)
終端後 (4)
次の処理へ (6)
UDP終端処理プロトコル (7)
ヘッダ部分の更新 (9)
終端後 (8)
次の処理へ (10)
L2TP終端処理プロトコル (11)
ヘッダ部分の更新 (13)
終端後 (12)
次の処理へ (14)
PPP終端処理プロトコル (15)
ヘッダ部分の更新 (17)
終端後 (16)
(18)
IP(a→b) (19) 終端処理プロトコル
終了処理(ヘッダの除去) (20)
処理後のパケット (21)
ペイロード

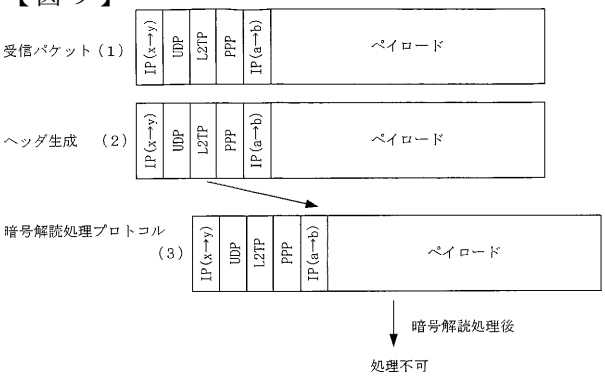
【図７】


受信パケット (1)
ヘッダ生成 (2)
デコード
IP(x→y)の終端処理 (3) プロトコル
ヘッダ部分の更新 (5)
終端後 (4)
次の処理へ (6)
UDP終端処理プロトコル (7)
ヘッダ部分の更新 (9)
終端後 (8)
次の処理へ (10)
L2TP終端処理プロトコル (11)
ヘッダ部分の更新 (13)
終端後 (12)
次の処理へ (14)
PPP終端処理プロトコル (15)
ヘッダ部分の更新 (17)
終端後 (16)
終了処理(ヘッダの除去) (18)
処理後のパケット (19)
ペイロード

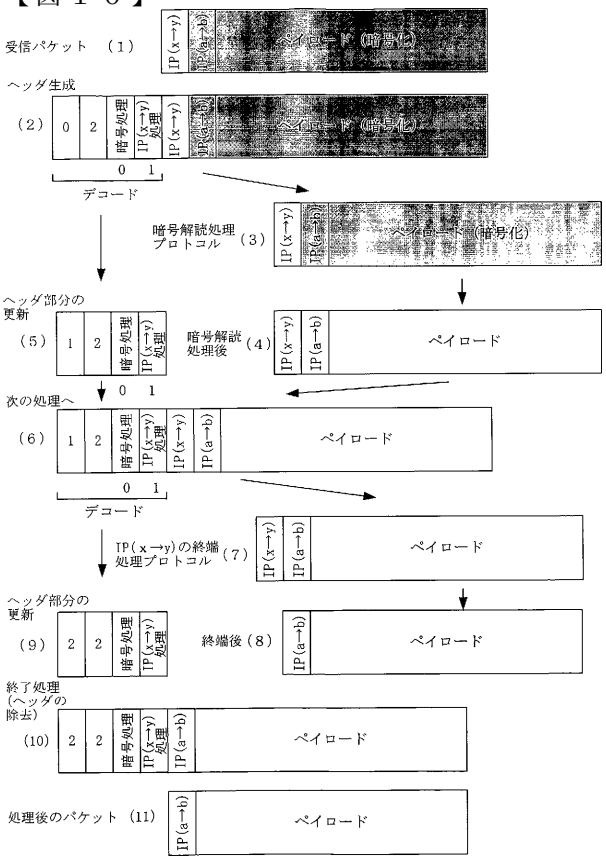
【図８】


受信パケット (1)
ヘッダ生成 (2)
IP(x→y)の終端処理プロトコル (3)
終端後 (4)
次の処理へ (5)
UDP終端処理プロトコル (6)
ペイロード(暗号化)
処理不可

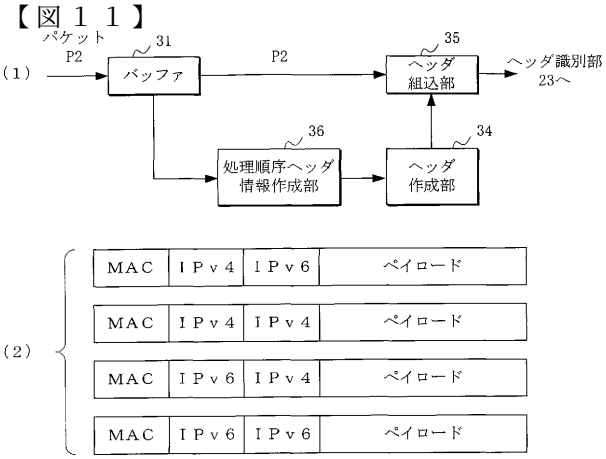
【図９】



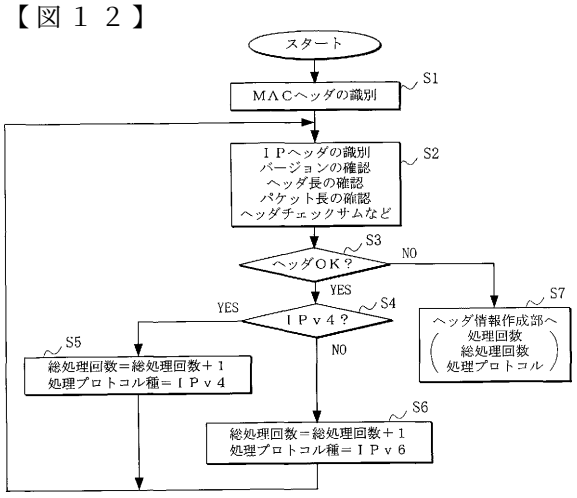
【図１０】



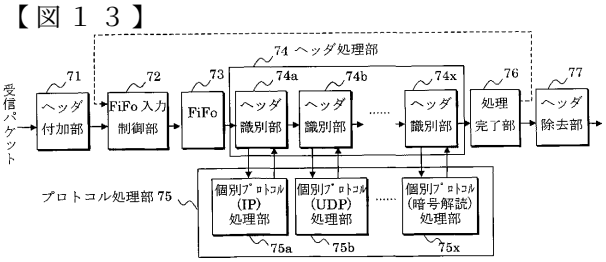
【図１１】



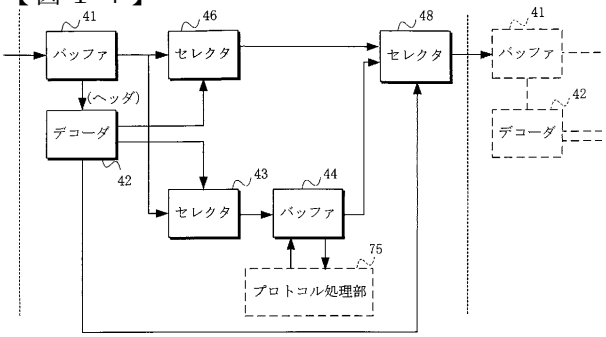
【図１２】



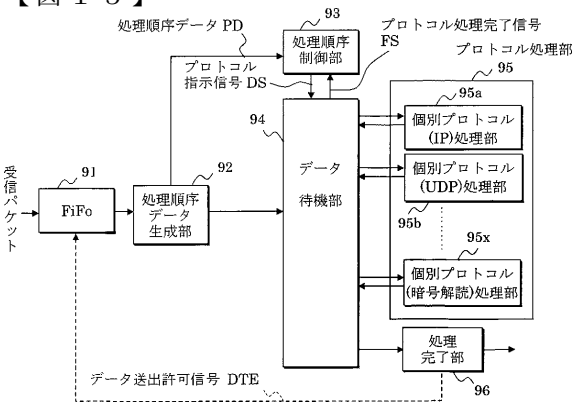
【図１３】



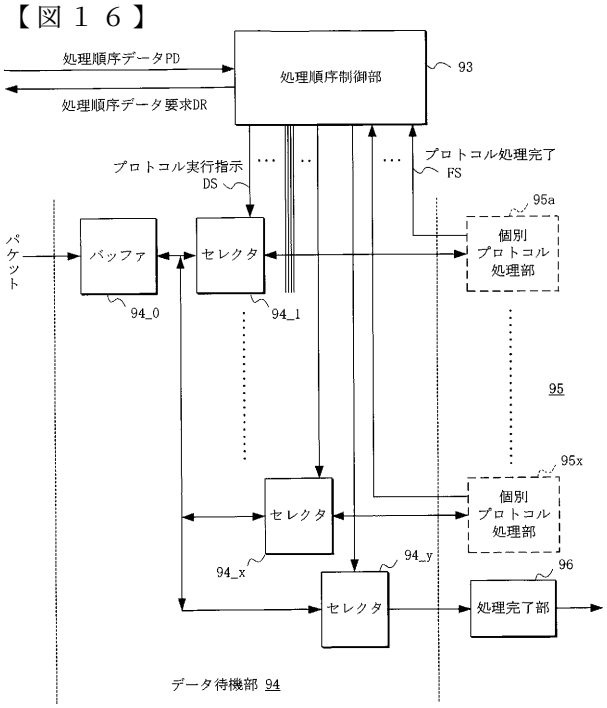
【図１４】



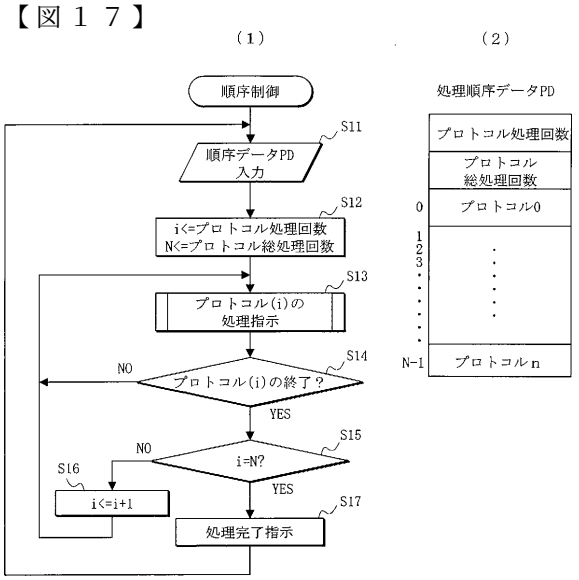
【図１５】



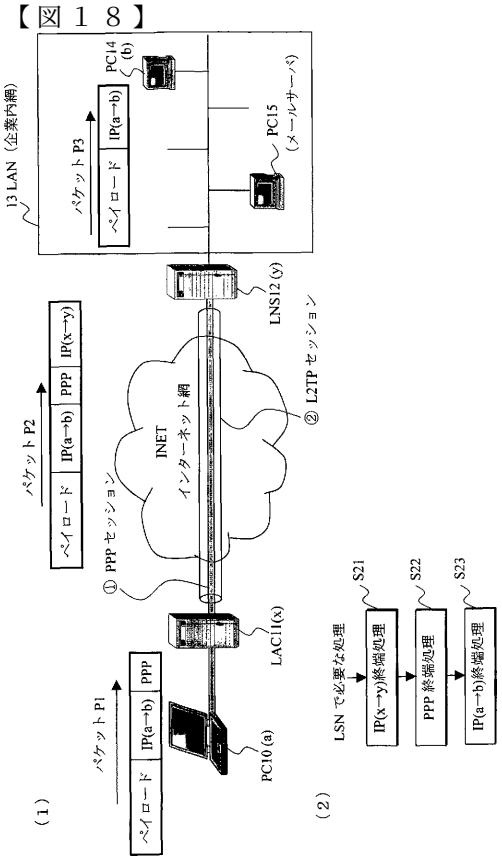
【図１６】



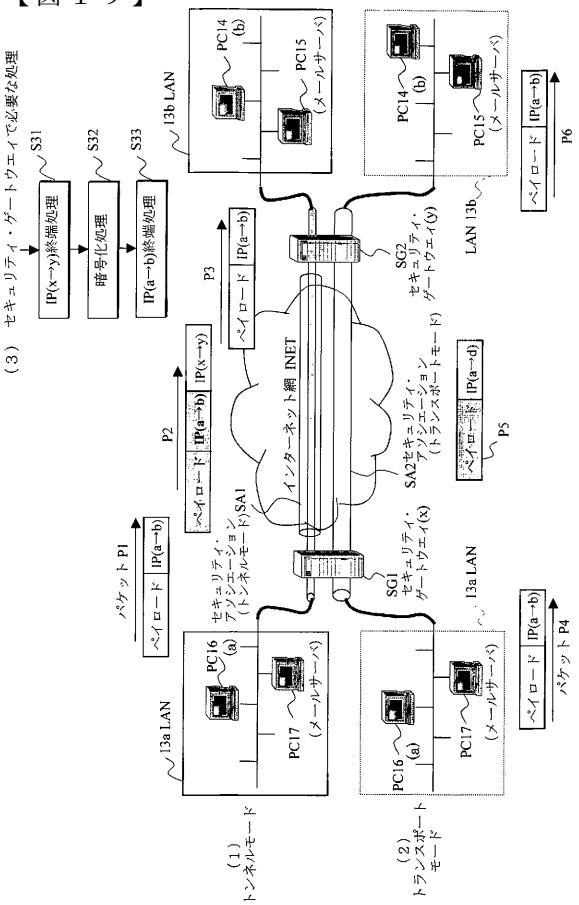
【図１７】



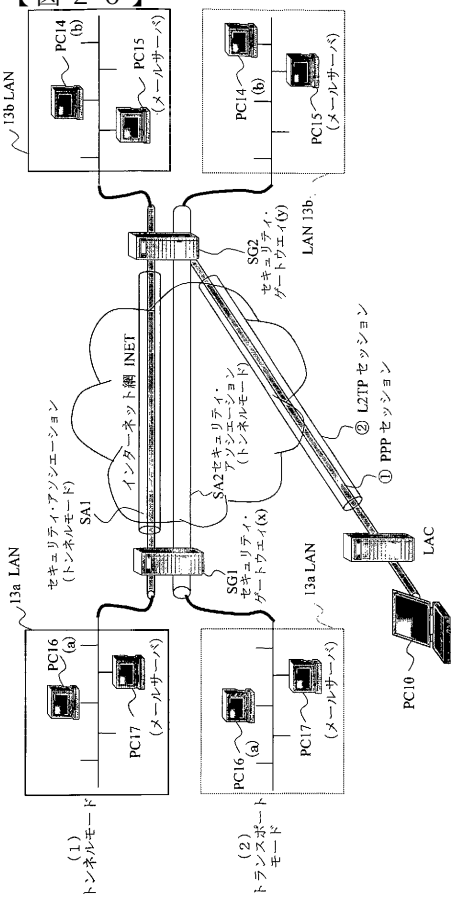
【図１８】



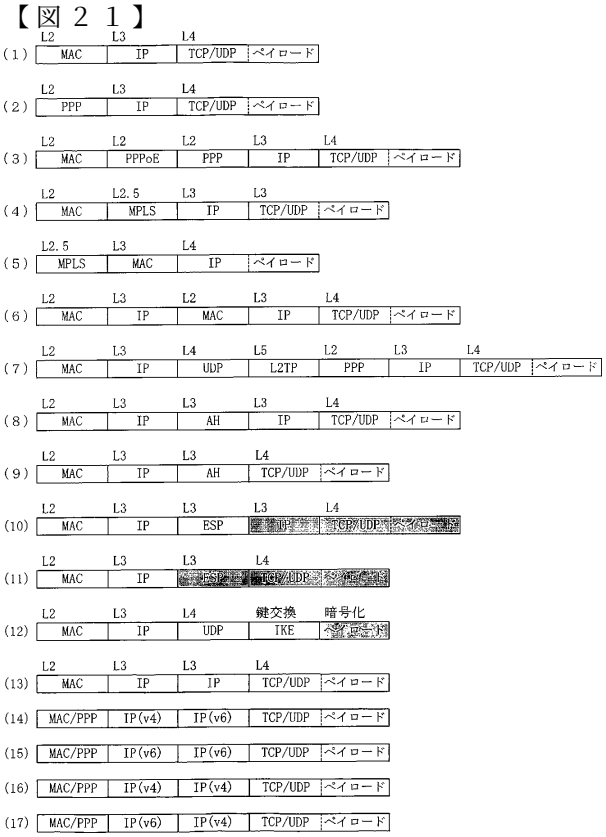
【図１９】



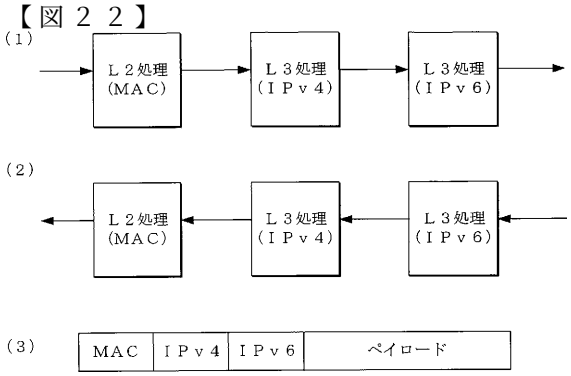
【図２０】



【図２１】



【図２２】



フロントページの続き

(72)発明者　中村　正和
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内
(72)発明者　三田　浩一
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内
(72)発明者　新井　隆
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内
(72)発明者　渡邊　秀明
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内
(72)発明者　三島　一乃
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内
(72)発明者　廣井　竜一
神奈川県横浜市港北区新横浜２丁目３番９号　富士通ディジタル・テクノロジ株式会社内

審査官　安藤　一道

(56)参考文献　特開平１１－３１７７８３（ＪＰ，Ａ）
特開平０８－１９５７８３（ＪＰ，Ａ）
特開平０８－０８８６６６（ＪＰ，Ａ）