(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第3599552号

(P3599552)

(45)発行日　平成16年12月8日(2004.12.8)　(24)登録日　平成16年9月24日(2004.9.24)

(51)Int.Cl.[7]	F I		
H04L 12/66	H04L	11/20	B
G09C 1/00	G09C	1/00	660E
H04L 9/32	H04L	9/00	675A
H04L 12/56	H04L	11/20	102A

請求項の数 11　(全 17 頁)

(21)出願番号　特願平10-7682
(22)出願日　平成10年1月19日(1998.1.19)
(65)公開番号　特開平11-205388
(43)公開日　平成11年7月30日(1999.7.30)
審査請求日　平成13年8月15日(2001.8.15)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100084032
弁理士　三品　岩男
(72)発明者　橋本　和夫
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　西門　隆
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

最終頁に続く

(54)【発明の名称】パケットフィルタ装置、認証サーバ、パケットフィルタリング方法及び記憶媒体

(57)【特許請求の範囲】

【請求項１】

ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置であって、

前記公衆網に接続される公衆接続部と、

前記私設網に直接接続される私設接続部と、

前記ファイアウォールに接続されるファイアウォール接続部と、

前記私設接続部で受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆接続部から前記公衆網に送信し、前記ファイアウォール接続部で受信したデータパケットを前記公衆接続部から前記公衆網に送信するパケット転送手段と、

前記公衆接続部で受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断し、前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設接続部から当該データパケットを送信し、前記認証情報が付加されたデータパケットでなければ前記ファイアウォール接続部から当該データパケットを送信するパケット振り分け手段と

を有することを特徴とするパケットフィルタ装置。

【請求項２】

請求項1に記載のパケットフィルタ装置において、

前記認証情報に対応する認証キー情報を記憶する認証キー記憶手段と、

前記認証キー情報を、前記認証キー記憶手段に設定する認証キー設定手段と

をさらに有することを特徴とするパケットフィルタ装置。
【請求項３】
請求項２に記載のパケットフィルタ装置において、
前記パケット転送手段は、
前記認証キー記憶手段に記憶する認証キー情報から前記認証情報を作成する作成手段と、
前記作成手段により作成された認証情報を前記データパケットのあらかじめ定めた領域に付加する付加手段と
を備えることを特徴とするパケットフィルタ装置。
【請求項４】
請求項２に記載のパケットフィルタ装置において、
前記パケット振り分け手段は、
前記データパケットから認証情報を抽出し、当該認証情報が、前記認証キー記憶手段に記憶する認証キー情報から作成した認証情報と一致するかいなかを判断する検査手段と、
前記検査手段により、一致する認証情報が付加されたデータパケットであれば、当該認証情報を取り除く削除手段と
を備えることを特徴とするパケットフィルタ装置。
【請求項５】
請求項1に記載のパケットフィルタ装置において、
複数のプライベートネットに対応する前記私設接続部を複数備え、
前記パケット転送手段は、前記複数のプライベートネットワークの各々に対応する認証情報を付加し、
前記パケット振り分け手段は、前記複数のプライベートネットワークの各々に対応する認証情報から、当該認証情報に対応する前記私設接続部を判断し、対応する私設接続部から当該データパケットを送出することを特徴とするパケットフィルタ装置。
【請求項６】
請求項５に記載のパケットフィルタ装置において、
複数のプライベートネットに対応する前記公衆接続部を複数備えることを特徴とするパケットフィルタ装置。
【請求項７】
請求項５または６に記載のパケットフィルタ装置において、
前記複数のプライベートネットワークの各々に対応する認証情報に対応する認証キー情報を各々記憶する認証キー記憶手段と、
前記認証キー情報の各々を、前記認証キー記憶手段に設定する認証キー設定手段と
をさらに有することを特徴とするパケットフィルタ装置。
【請求項８】
パケットの送信元に従ってパケットを振り分けるパケットフィルタ装置であって、
前記送信元からパケットを受信するための第１の接続部と、
前記パケットを出力する第２および第３の接続部と、
前記第１の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかないかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第２の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第３の接続部から当該データパケットを送信させるパケット振り分け手段と
を有し、
前記第２および第３の接続部は、
パケットをさらに受信し、前記第２の接続部で受信したパケットにあらかじめ定めた送信元情報を付加して前記第１の接続部から当該パケットを送信し、前記第３の接続部で受信したパケットはそのまま第１の接続部から送信させるパケット転送手段を有することを特徴とするパケットフィルタ装置。
【請求項９】

私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置に対して、当該パケットフィルタ装置におけるパケット振り分けのための認証キー情報を送信する認証サーバであって、
前記パケットフィルタ装置が当該認証サーバへのアクセスが正当であるかないかを判断する判断手段と、
前記判断手段により正当と判断されたパケットフィルタ装置に対して前記プライベートネットワークに対応する認証キー情報を送信する送信手段と
を備えることを特徴とする認証サーバ。
【請求項１０】
ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタリング方法であって、
前記私設網から受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆網に送信するステップと、
前記ファイアウォールから受信したデータパケットを前記公衆網に送信するステップと、
前記公衆網から受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断するステップと、
前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設網へ当該データパケットを送信するステップと、
前記認証情報が付加されたデータパケットでなければ前記ファイアウォールへ当該データパケットを送信するステップと
を備えることを特徴とするパケットフィルタリング方法。
【請求項１１】
請求項１０に記載のステップを情報処理装置により実現するためのプログラムを記憶する記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、通信網間を接続してデータパケットをフィルタリングする技術に係り、特に、アプリケーション毎のチェック機能を有するファイアウォールと連携して高速で且つ安全性の高いパケットフィルタリング方法及びその装置を提供するものである。
【０００２】
【従来の技術】
近年、公衆網を用いて私設網をそれぞれ接続し、私設網の広域化を実現するインターネットＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）の構築が盛んになりつつある。私設網を公衆網に接続させる場合、公衆網での盗聴及び不正アクセスにさらされる危険性があり、セキュリティ面で大きな問題点がある。
【０００３】
このような問題点に対して、各ユーザが、暗号化手段やアクセス制御手段をもつファイアウォールを導入してセキュリティ面でのリスクをできる限り小さくすることが可能である。既に、各社より暗号化手段を備えたファイアウォールが出荷されている。例えば、日経コミュニケーション１９９６．６．１７　Ｎｏ．２２４の８６頁～１００頁にインターネットＶＰＮが紹介されている。
【０００４】
このインターネットＶＰＮについて図１２を参照して説明する。
【０００５】
図１２において、私設網Ａ１０１－１と私設網Ｂ１０１－２とは、それぞれの私設網内に設置されたファイアウォールＡ１０６－１及びファイアウォールＢ１０６－２を介して公衆網１０３にそれぞれ接続される。ファイアウォールＡ１０６－１及びファイアウォールＢ１０６－２は、暗号化手段を備える不正アクセスを防ぐためのゲートウエイ装置である

。
【０００６】
例えば、計算機Ａ１０４－１が計算機Ｂ１０４－２と通信する場合、以下の手順で行われる。
【０００７】
計算機Ａは、計算機Ｂに対してデータパケットの送信を行う。送信されたデータパケットは、ヘッダ部にあらかじめ定められた送信元アドレス及びポート番号が書かれており、ファイアウォールＡで暗号化されて公衆網に送信される。
【０００８】
暗号化されたデータパケットは、公衆網を介してファイアウォールＢに送られる。
【０００９】
ファイアウォールＢでは、データパケットの復号化を行う。また、データパケットのヘッダ部に書かれた送信元アドレス及びポート番号よりアクセス権限をチェックして、アクセス可能な計算機と判断した場合、データパケットを計算機Ｂに送信する。不正なアクセスと判断した場合、計算機Ｂにはデータパケットを送らない。
【００１０】
次に、図１３を参照してファイアウォール１０６の内部構成を説明する。図１３に、ファイアウォール１０６の内部構成図を示す。図１３において、ファイアウォール１０６は、ネットワークに接続される入出力手段１３０１、暗号化および復号化を行う暗号化手段１３０２、不正アクセスを防ぐためのコネクション管理手段１３０３、及び、アプリケーション毎のアクセスを管理するためのアプリケーション管理手段１３０４を備える。コネクション管理手段及びアプリケーション管理手段は、参照テーブルとして、アクセス可能な、送信元の計算機のアドレスおよびポート番号を記憶するコネクション管理テーブルＡ１３０５、及び、アプリケーションプロトコル毎に定義されたアクセス可能な計算機のアドレスを記憶するコネクション管理テーブルＢ１３０６を備えている。
【００１１】
入出力手段１３０１は、データパケット１３０７を通信網からファイアウォール内部に入力し、又、通信網上に出力する手段である。
【００１２】
暗号化手段１３０２は、ペイロード１３０７－２の暗号化、復号化を行う手段である。
【００１３】
コネクション管理手段１３０３は、ヘッダ１３０７－１に書かれたポート番号及び送信元アドレスから、コネクション管理テーブルＡ１３０５に書かれたアクセス可能な計算機か否かを判断する手段である。
【００１４】
アプリケーション管理手段１３０４は、アプリケーションプロトコル毎に定義されたアクセス制御情報に基づいてアクセス可能な計算機かどうかを判断する手段である。データパケット１３０７のペイロード１３０７－２に書かれたアクセス制御情報からコネクション管理テーブルＢ１３０６に書かれたアクセス可能な計算機か否かを判断する。なお、アプリケーション管理手段は、アプリケーションプロトコル毎に仕様が異なっており、ファイアウォールがサポートするアプリケーションプロトコルの数だけ備えることができる。
【００１５】
【発明が解決しようとする課題】
上述した従来技術を用いて、ファイアウォールによるデータパケットの暗号化及びアクセス制御を行うことで公衆網を使ったインターネットＶＰＮを構築することは可能である。しかし、ファイアウォールには、以下に示すような問題がある。
【００１６】
アプリケーションプロトコル毎にコネクションを管理する方法は、高いセキュリティを確保できる反面、アプリケーションプロトコル毎にそれぞれ異なる対応をしなければならない。通常、複数のアプリケーションが通信網を利用するため、ファイアウォールはそれら

全てに対応しなければならず、処理が煩雑になる。結果として、処理時間がかかってしまう。例えば、前述したインターネットＶＰＮを利用する際に、インターネットＶＰＮに接続されていない計算機とも通信を行う場合には、ファイアウォールでは、インターネットＶＰＮに接続されている計算機であるか、否かに関わらず、前述した、すべてのアプリケーションについてのアクセス権限のチェックを行う。この処理に時間がかかっている。

【００１７】

一方、インターネットＶＰＮを、公衆網側でサービスとして提供されることが望まれている。この場合、既存の設備を利用しつつ、新たなサービスを受けられることが望ましい。

【００１８】

そこで、本発明は、処理速度の高速化を図り、高いセキュリティを確保できるインターネットＶＰＮのサービスを提供するためのパケットフィルタ装置、認証サーバ、パケットフィルタリング方法及び記憶媒体を提供することを目的とする。

【００１９】

【課題を解決するための手段】

本発明は、処理速度の高速化と、高いセキュリティを確保したインターネットＶＰＮを提供するため、以下の手法を用いる。

【００２０】

ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置であって、

前記公衆網に接続される公衆接続部と、

前記私設網に直接接続される私設接続部と、

前記ファイアウォールに接続されるファイアウォール接続部と、

前記私設接続部で受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆接続部から前記公衆網に送信し、前記ファイアウォール接続部で受信したデータパケットを前記公衆接続部から前記公衆網に送信するパケット転送手段と、

前記公衆接続部で受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断し、前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設接続部から当該データパケットを送信し、前記認証情報が付加されたデータパケットでなければ前記ファイアウォール接続部から当該データパケットを送信するパケット振り分け手段とを有する。

【００２１】

前記認証情報に対応する認証キー情報を記憶する認証キー記憶手段と、前記認証キー情報を、前記認証キー記憶手段に設定する認証キー設定手段とをさらに有する。前記パケット転送手段は、前記認証キー記憶手段に記憶する認証キー情報から前記認証情報を作成する作成手段と、前記作成手段により作成された認証情報を前記データパケットのあらかじめ定めた領域に付加する付加手段とを備える。

【００２２】

前記パケット振り分け手段は、前記データパケットから認証情報を抽出し、当該認証情報が、前記認証キー記憶手段に記憶する認証キー情報から作成した認証情報と一致するかいなかを判断する検査手段と、前記検査手段により、一致する認証情報が付加されたデータパケットであれば、当該認証情報を取り除く削除手段とを備える。

【００２３】

複数のプライベートネットに対応する前記私設接続部を複数備え、

前記パケット転送手段は、前記複数のプライベートネットワークの各々に対応する認証情報を付加し、

前記パケット振り分け手段は、前記複数のプライベートネットワークの各々に対応する認証情報から、当該認証情報に対応する前記私設接続部を判断し、対応する私設接続部から当該データパケットを送出する。また、複数のプライベートネットに対応する前記公衆接続部を複数備えることを特徴とするパケットフィルタ装置。

【００２４】

前記複数のプライベートネットワークの各々に対応する認証情報に対応する認証キー情報を各々記憶する認証キー記憶手段と、前記認証キー情報の各々を、前記認証キー記憶手段に設定する認証キー設定手段とをさらに有するようにしてもよい。

【００２５】

また、パケットの送信元に従ってパケットを振り分けるパケットフィルタ装置であって、
前記送信元からパケットを受信するための第１の接続部と、
前記パケットを出力する第２および第３の接続部と、
前記第１の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかないかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第２の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第３の接続部から当該データパケットを送信させるパケット振り分け手段とを有する。前記第２および第３の接続部は、パケットをさらに受信し、
前記第２の接続部で受信したパケットにあらかじめ定めた送信元情報を付加して前記第１の接続部から当該パケットを送信し、前記第３の接続部で受信したパケットはそのまま第１の接続部から送信させるパケット転送手段をさらに有する。

【００２６】

ハードウエア構成としては、
前記送信元からパケットを受信するための第１の接続部と、
前記パケットを出力する第２および第３の接続部と、
処理を行うＣＰＵと、
前記第１の接続部で受信したパケットがあらかじめ定めた送信元から送信されたパケットであるかないかを判断し、前記あらかじめ定めた送信元からのパケットであれば、前記第２の接続部から当該データパケットを送信し、前記あらかじめ定めた送信元からのパケットでなければ前記第３の接続部から当該データパケットを送信させるためのプログラムを記憶するメモリとを有する。

【００２７】

また、私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタ装置に対して、当該パケットフィルタ装置におけるパケット振り分けのための認証キー情報を送信する認証サーバであって、
前記パケットフィルタ装置が当該認証サーバへのアクセスが正当であるかないかを判断する判断手段と、
前記判断手段により正当と判断されたパケットフィルタ装置に対して前記プライベートネットワークに対応する認証キー情報を送信する送信手段とを備える。

【００２８】

ファイアウォールを備える私設網に接続され、公衆網を介してのプライベートネットワークを構成させるためのパケットフィルタリング方法であって、
前記私設網から受信したデータパケットにあらかじめ定めた認証情報を付加して前記公衆網に送信するステップと、
前記ファイアウォールから受信したデータパケットを前記公衆網に送信するステップと、
前記公衆網から受信したデータパケットが、前記認証情報が付加されたデータパケットであるかないかを判断するステップと、
前記認証情報が付加されたデータパケットであれば、当該認証情報を取り除き、前記私設網へ当該データパケットを送信するステップと、
前記認証情報が付加されたデータパケットでなければ前記ファイアウォールへ当該データパケットを送信するステップとを備える。これらのステップを情報処理装置により実現するためのプログラムは、記憶媒体に記憶しておくことができる。
以上の動作により、ＶＰＮを構成する私設網間のデータパケットは、セキュリティが保証できる。また、パケットフィルタ装置が付加する認証情報は、アプリケーションプロトコルに係わらず一定であるためハードウェアによる高速化が可能であり、高速なアクセス制御が行える。更に私設網内のあるＷＷＷサーバへのアクセスを許す場合や、逆に私設網か

ら公衆網上のWWWサーバをアクセスする際等、ＶＰＮ外の情報処理装置へのアクセスはファイアウォールを経由して行えるので、速度は私設接続部より落ちるが、細やかなセキュリティの実現が可能である。

【００２９】

なお、公衆網とパケットフィルタ装置の間は一つの回線で接続されるため、専用線と一般公衆線を分けずに一つの回線契約で実現できるという利点もある。

【００３０】

【発明の実施の形態】

以下、図面を参照して、本発明の実施の形態を詳しく説明する。

【００３１】

図１は、本発明の一実施の形態であるシステム構成図を示している。図１において、本システム構成では、私設網Ａ１０１－１、私設網Ｂ１０１－２及び私設網Ｃ１０１－３が存在する。私設網Ａ及び私設網Ｂは、公衆網１０３を介してＶＰＮを構成する私設網の対とし、私設網Ｃは、公衆網１０３を介して他の私設網とＶＰＮを構成しない私設網とする。

【００３２】

公衆網には、私設網Ａ及び私設網Ｂ　のＶＰＮを構成させるため、パケットフィルタ装置Ａ１０２－１を設け、私設網Ａに接続させる。私設網Ｂと公衆網との接続点にも同様に、パケットフィルタ装置Ｂ１０２－２を設ける。私設網Ｃは、他とＶＰＮを構成しないため、パケットフィルタ装置を必要としない。

【００３３】

私設網Ａとパケットフィルタ装置Ａとの接続には、二経路を設ける。一経路は、パケットフィルタ装置Ａと内部ルータＡ１０５－１とを直接接続させる直結経路１０７－１であり、もう一経路は、ファイアウォールＡ１０６－１を経由して内部ルータＡに接続させるファイアウォール経路１０８－１である。計算機Ａ１０４－１は、内部ルータＡに接続される。私設網Ｂとパケットフィルタ装置Ｂとの接続方法も、私設網Ａとパケットフィルタ装置Ａの接続と同様である。

【００３４】

私設網Ｃは、パケットフィルタ装置が存在しないため、ファイアウォールＣ１０６－３を介して公衆網と接続される。計算機Ｃは、ファイアウォールＣに接続される。

【００３５】

また、パケットフィルタ装置計算機１０９は、パケットフィルタの機能を内蔵する計算機である。

【００３６】

なお、図１では直結経路１０７、ファイアウォール経路１０８ともに物理的な通信線のイメージで説明したが、ＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ　Ｔｒａｎｓｆｅｒ　Ｍｏｄｅ）のように一本の物理的な通信線の上に実現された論理的な通信線を経路と考えてもよい。

【００３７】

図２は、パケットフィルタ装置１０２の内部構成を示している。パケットフィルタ装置は、公衆網側に設置され、私設網から送信されるデータパケットに認証情報を付加し、又、公衆網から受信したデータパケットをファイアウォールに振り分けたり、付加された認証情報をチェックする装置である。

【００３８】

パケットフィルタ装置は、パケット転送手段２０１、パケット振り分け手段２０２、認証キー記憶手段２０３及び認証キー設定手段２０４を備える。また、パケットフィルタ装置は、直結経路１０７、ファイアウォール経路１０８、及び、公衆網１０３の三つの入出力回線を持っている。

【００３９】

パケット転送手段２０１は、直結経路１０７から受信した、計算機からのデータパケットに対して、認証情報を付加して公衆網１０３に送信し、また、ファイアウォール経路１０

８から受信した、計算機からのデータパケットに対して、そのまま公衆網に送信する。

【００４０】

パケット振り分け手段２０２は、公衆網１０３から受信したデータパケットに対して、データパケットの特定位置にある、他のパケットフィルタ装置で付加された認証情報が付加されているか否かを判断して、認証情報が付加されているデータパケットに対しては認証情報を検査し、正しい認証情報が付加されていれば、ＶＰＮにおけるデータパケットであるとして直結経路１０７に送信し、認証情報が付加されていないか、或いは、正しい認証情報でないデータパケットに対してはファイアウォール経路１０８に送信する。

【００４１】

認証キー記憶手段２０３は、認証情報を作成し、または、検査する時に参照する認証キーを記憶するメモリである。

【００４２】

認証キー設定手段２０４は、認証キーをパケットフィルタ装置の認証キー記憶手段２０３に設定するためのユーザインタフェースである。

【００４３】

本実施の形態では、私設網Ａ及び私設網ＢはＶＰＮを構成するため、認証キー設定手段により、パケットフィルタ装置Ａ１０２－１及びパケットフィルタ装置Ｂ１０２－２の認証キー記憶手段２０３には共通の認証キーが設定されている。このように、ＶＰＮを構成する私設網に接続されるパケットフィルタ装置の認証キー記憶手段２０３には共通の認証キーを設定しておく。

【００４４】

つぎに、パケット転送手段２０１について詳細に説明する。図３は、パケット転送手段２０１の詳細な構成図を示している。図３において、パケット転送手段２０１は、経路判定手段３０１、認証情報作成手段３０２及び認証情報付加手段３０３を備える。

【００４５】

経路判定手段３０１は、直結経路１０７から受信したデータパケットか、或いは、ファイアウォール経路１０８から受信したデータパケットかを受信したポートにより判定し、直結経路から受信したデータパケットは、認証情報作成手段３０２及び認証情報付加手段３０３を経由させて公衆網１０３に送信し、ファイアウォール経路から受信したデータパケットは、そのまま公衆網に送信する。

【００４６】

認証情報作成手段３０２は、経路判定手段３０１から受け取ったデータパケットと、認証キー記憶手段２０３に記憶されている認証キーとから認証情報を作成する。本実施の形態では、暗号学で既に知られているハッシュ関数を用いて認証情報を作成する。

【００４７】

認証情報付加手段３０３は、認証情報作成手段３０２により作成された認証情報をデータパケットのあらかじめ定められた特定領域に付加する。

【００４８】

次に、図２に示すパケット振り分け手段２０２の構成を詳細に説明する。図４は、パケット振り分け手段２０２の詳細な構成図を示している。図４において、パケット振り分け手段２０２は、パケット判定手段４０１、認証情報検査手段４０２及び認証情報削除機能４０３を備える。

【００４９】

パケット判定手段４０１は、公衆網１０３から受信したデータパケットに対して特定領域に認証情報が付加されているか否かを判断し、認証情報が付加されているデータパケットは、認証情報検査手段４０２及び認証情報削除手段４０３を経由させて直結経路１０７に送信し、認証情報が付加されていない、或いは、正しい認証情報でないデータパケットは、ファイアウォール経路１０８に送信する。

【００５０】

認証情報検査手段４０２は、認証情報が正しいか否かを判定する。この場合、パケット判

定手段４０１から受け取ったデータパケットと、認証キー記憶手段２０３に記憶されている認証キーとから新たに認証情報を作成し、データパケットに付加されている認証情報と一致するかいなかを比較する。一致する場合、正しい認証情報と判定し、一致しない場合、正しい認証情報でないと判定する。

【００５１】

認証情報削除手段４０３は、正しい認証情報と判定されたデータパケットに挿入されている認証情報を削除する。

【００５２】

認証情報は、図５に示すデータパケットの特定の位置に挿入されている。図５は、データパケットのフォーマットを示している。データパケットは、送信先アドレス５０１、送信元アドレス５０２及びポート番号５０３が記述されたヘッダ１３０７－１と、データが記述されたペイロード１３０７－２とから構成される。本実施の形態では、認証情報を、例えば標準通信プロトコルＩｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ　Ｖｅｒｓｉｏｎ６（ＩＰｖ６）で規定されているフォーマットに従って、データパケットに挿入する。ＩＰｖ６では、ヘッダ１３０７－１とペイロード１３０７－２との間に任意の制御データ５０４を、制御データのサイズや種別を区別する制御ヘッダと共に挿入できるよう規定されており、これを利用して認証情報用の制御ヘッダ５０５と共に認証情報５０６を挿入することで、認証情報の有無を判断できる。

【００５３】

次に、図６および図７を参照して本実施の形態における処理動作を説明する。図６および図７は、本実施の形態の構成における処理シーケンスを示している。ここでは、図１に示す私設網Ａ１０１－１内の計算機Ａ１０４－１が、ＶＰＮを構成する私設網Ｂ１０１－２内の計算機Ｂ１０４－２に通信を行う場合の手順について説明する。図６に、送信側の処理を示し、図７に受信側の処理を示す。

【００５４】

（１）計算機Ａ１０１－１は、送信先アドレスを、私設網Ｂ１０１－２内の計算機Ｂ１０４－２にして、データパケットを送信する（図６に示す手順２０００）。

【００５５】

（２）内部ルータＡ１０５－１は、データパケットのヘッダに記述された送信先アドレスをチェックする。送信先アドレスが、私設網Ａ１０１－１とＶＰＮを構成する私設網である場合、直結経路を使ってデータパケットをパケットフィルタ装置Ａ１０２－１に送信する（手順２００１）。その他の送信先アドレスの場合には、ファイアウォールに送信し、セキュリティチェックを行った後、ファイアウォール経路でデータパケットをパケットフィルタ装置Ａに送信する（手順２００２）。

【００５６】

（３）パケットフィルタ装置Ａは、直結経路から受信したデータパケットに対して、図３に示す認証情報作成手段３０２及び認証情報付加手段３０３を用いて認証情報をデータパケットに付加し、公衆網１０３に送信する（手順２００３）。ファイアウォール経路から受信したデータパケットに対しては、そのまま公衆網に送信する（手順２００４）。

【００５７】

（４）受信側のパケットフィルタ装置Ｂ１０２－２は、公衆網１０３からデータパケットを受信する（図７に示す手順２００５）。

【００５８】

（５）パケットフィルタ装置Ｂ１０２－２は、パケット判定手段４０１を用いてデータパケットに認証情報が付加されているか否かを判断する。認証情報が付加されている場合、認証情報検査手段４０２を用いて認証情報が正しいか否かを判断し、認証情報削除手段４０３を用いて認証情報を削除する（手順２００６）。認証情報が正しい場合は、直結経路を経由して内部ルータＢ１０５－２にデータパケットを送信する（手順２００７）。認証情報が付加されていない、或いは、正しい認証情報でない場合は、ファイアウォール経路を経由してファイアウォールＢ１０６－２にデータパケットを送信する（手順２００８）

。
【００５９】
（６）ファイアウォールＢ１０６－２は、ファイアウォール経路を経由して送信されたデータパケットに対して詳細なセキュリティチェックを行った後、内部ルータＢ１０５－２にデータパケットを送信する（手順２００９）。
【００６０】
（７）計算機Ｂ１０４－２は、内部ルータＢからデータパケットを受信する（手順２０１０）。
【００６１】
上述した図１～図７に示す実施の形態では、私設網間を公衆網に接続して通信する場合を説明している。携帯端末等を公衆網に直接接続するような場合には、携帯端末にパケットフィルタ装置と同等の機能をソフトウェア、或いは、ハードウェアとして提供することで本実施の形態を実現することができる。すなわち、上述した機能は、ソフトウエアにより実現することができる。
【００６２】
パケットフィルタ装置のハードウエア構成を図１４に示す。図１４において、パケットフィルタ装置は、公衆網に接続される公衆網接続部１４５０と、私設網に直接接続される私設網接続部１４１０と、ファイアウォールに接続されるファイアウォール接続部１４２０と、処理を行うＣＰＵ１４３０と、公衆網接続部１４５０で受信したパケットがあらかじめ定めた送信元から送信されたパケット（認証情報が付加されたパケット）であるかないかを判断し、あらかじめ定めた送信元からのパケットであれば、私設網接続部１４１０から当該データパケットを送信し、あらかじめ定めた送信元からのパケットでなければファイアウォール接続部１４２０から当該データパケットを送信させるためのプログラムを記憶するメモリ１４４０とを有する。さらに、メモリ１４４０は、私設網接続部１４１０で受信したパケットにあらかじめ定めた送信元情報（認証情報）を付加して公衆網接続部１４５０から当該パケットを送信し、ファイアウォール接続部１４２０で受信したパケットはそのまま公衆網接続部１４５０から送信させるプログラムを備える。
【００６３】
本実施の形態によれば、パケットフィルタ装置により、ＶＰＮのサービスを網側で提供することができる。また、ＶＰＮを構成する私設網間の通信は、セキュリティを守りつつ、リアルタイムデータの転送を実現することができる。ＶＰＮ以外の通信は、ファイアウォールによる細やかなセキュリティが実現できる。
【００６４】
つぎに、第２の実施の形態について説明する。
【００６５】
第１の実施の形態では、各私設網が一つのＶＰＮグループにのみ属する例を考えてきた。しかし、一つの私設網が、複数のＶＰＮグループに属する場合も考えられる。例えば、図１に示す私設網Ａと私設網Ｂとで第１のグループを作り、私設網Ａと私設網とＣで別の第２のグループを作るような場合である。この場合、グループ毎に異なる認証キーを持つことで、どのグループに属するデータパケットかを区別することができる。第２の実施の形態では、第１の実施の形態と同様な構成で、認証キーをＶＰＮグループごとに設けて、各々の認証を行う。
【００６６】
第２の実施の形態における認証キーについて図８を参照して説明する。図８は、認証キー記憶手段２０３として単に一つの認証キーを記憶するのではなく、複数の認証キーを管理する方法について示した説明図である。本実施の形態では、ＶＰＮグループに属する私設網のアドレス群と、認証キーとを対にして記憶する。対の数は、私設網が属するＶＰＮグループの数に一致する。
【００６７】
認証情報作成手段３０２では、ヘッダ１３０７－１に記述された送信先アドレスから、ま

た認証情報検査手段４０２では、ヘッダ１３０７－１に記述された送信元アドレスからＶＰＮグループに対応した認証キーを検索して認証情報の作成、或いは、検査を行う。

【００６８】

本実施の形態により、異なる認証キーを用いることでデータパケットがどのＶＰＮグループに属するかを判別することが可能となる。

【００６９】

次に、第３の実施の形態を説明する。第３の実施の形態では、ＶＰＮグループごとに、私設網１０１及びパケットフィルタ装置１０２を接続させる直結経路１０７を設ける場合について、図９を参照して説明する。

【００７０】

図９は、複数のＶＰＮグループに対応した認証キー管理方法について示した説明図である。

【００７１】

図９において、認証キー記憶手段２０３は、直結経路の番号に対応して認証キーを記憶する。内部ルータ１０５は、グループに対応した直結経路にデータパケットを送信する。認証情報作成手段３０２は、認証キー記憶手段２０３の情報を使ってデータパケットが送信された直結経路のポート番号から認証キーを検索し、認証情報を作成する。認証情報検査手段４０２は、認証キー記憶手段の情報を使って各直結経路に対応した認証キーから順に、或いは、並列に認証情報を検査し、一致する認証情報を見つける。パケット判定手段４０１は、対応する直結経路を求め、データパケットを振り分ける。

【００７２】

本実施の形態により、直結経路１０７と認証キーとは一対一に対応する。よって、パケット転送手段２０１は、認証キーを高速に検索できる。

【００７３】

次に第４の実施の形態について説明する。第４の実施の形態では、認証キー記憶手段２０３に記憶される認証キーを通信開始時に設定する場合について説明する。図１０は、認証キー記憶手段２０３に記憶される認証キーを通信開始時に設定する場合の構成図である。本実施の形態では、認証サーバ１００１を公衆網１０３上に設置する。認証サーバ１００１は、公衆網１０３に接続された全てのパケットフィルタ装置１０２が所有する認証キーを記憶した記憶手段１０１０と、パケットフィルタ装置１０２を認証するパケットフィルタ装置認証手段１０１１と、認証キーをパケットフィルタ装置１０２に送信する認証キー送信手段１０１２とを備える。

【００７４】

パケットフィルタ装置Ａ１０２－１の認証キー設定手段２０４－１は、認証キーを設定するために、認証サーバ１００１と以下の手続きを行う。

【００７５】

（１）公衆網１０３との最初の通信を開始する時に認証サーバ１００１と接続させる。パケットフィルタ装置Ａ１０２－１の認証キー設定手段２０４－１は、あらかじめパスワードを受け付けておく。

【００７６】

（２）パケットフィルタ装置認証手段１０１１は、あらかじめ定めたパスワードを交換することでパケットフィルタ装置Ａ１０２－１を認証する。

【００７７】

（３）認証キー送信手段１０１２は、記憶手段１０１０から認証キーを取り出して、パケットフィルタ装置Ａ１０２－１に送信する。

【００７８】

（４）受信した認証キーを認証キー記憶手段２０３－１に設定する。

【００７９】

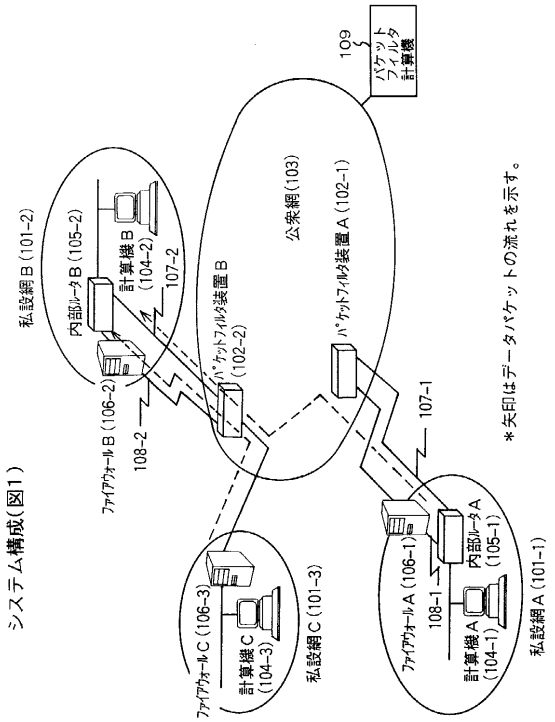
パケットフィルタ装置Ｂ１０２－２も同様の手続きを行い、認証キーを設定することができる。

【００８０】
本実施の形態により、認証キーの一元管理が可能となる。よって、認証キーの変更を行う場合、認証サーバ１００１上の一カ所で行うことができる。
【００８１】
つぎに、第５の実施の形態を説明する。第３の実施の形態では、公衆網１０３とパケットフィルタ装置１０２とを一つの経路で接続させた。しかし本実施の形態では、図１１に示す様に、複数の直結経路１０７及び一つのファイアウォール経路１０８に一対一で対応した経路で公衆網と、パケットフィルタ装置とを接続させる。すなわち、ＶＰＮごとに、直結経路１０７および公衆網とを設けておく。
【００８２】
パケット転送手段２０１は、直結経路を介して受信したデータパケットに対しては、直結経路に対応した認証情報を付加して、私設網側の直結経路に対応する公衆網側の経路に送信する。ファイアウォール経路を介して受信したデータパケットに対しては、そのまま私設網側のファイアウォール経路に対応する公衆網側の経路に送信する。
【００８３】
パケット振り分け手段２０２は、公衆網から受信したデータパケットをチェックし、正しい認証情報が付加されているデータパケットは、認証情報を取り除いて対応する直結経路に送信する。正しい認証情報が付加されていないデータパケットは、ファイアウォール経路に送信する。
【００８４】
本実施の形態により、パケット振り分け手段２０２は、経路により、ＶＰＮのグループの判別が容易になる。よって、パケット振り分け手段の高速化が可能となる。
【００８５】
上述した実施の形態によれば、パケットフィルタ装置が付加する認証情報は、アプリケーションプロトコルに係わらず一定であるため、ハードウェアによる実現が可能であり、高速なインターネットＶＰＮを実現できる。更に、私設網内のあるＷＷＷサーバへのアクセスを許す場合や、逆に私設網から公衆網上のＷＷＷサーバをアクセスする際等、ＶＰＮ外の情報処理装置へのアクセスはファイアウォールを経由して行えるので、速度は直結経路より落ちるが、細やかなセキュリティの実現が可能である。
【００８６】
【発明の効果】
本発明によれば、ＶＰＮを構成する私設網間の通信は、セキュアで且つリアルタイムデータの転送を可能とし、ＶＰＮ以外の通信は、ファイアウォールによる細やかなセキュリティが実現できる。
【図面の簡単な説明】
【図１】本発明の実施の形態におけるシステム構成図である。
【図２】本発明の実施の形態におけるパケットフィルタ装置の内部構成図である。
【図３】本発明の実施の形態におけるパケット転送手段の詳細を示す説明図である。
【図４】本発明の実施の形態におけるパケット振り分け手段の詳細を示す説明図である。
【図５】認証情報を付加したデータパケットの説明図である。
【図６】本発明の実施の形態における送信側の処理動作を示すシーケンス図である。
【図７】本発明の実施の形態における受信側の処理動作を示すシーケンス図である。
【図８】本発明の実施の形態における認証キー記憶手段の他の説明図である。
【図９】本発明の実施の形態における認証キー記憶手段の他の説明図である。
【図１０】本発明の実施の形態におけるシステム構成に認証サーバを追加した構成図である。
【図１１】パケットフィルタ装置の他の構成図である。
【図１２】ファイアウォールを用いた従来技術を示す構成図である。
【図１３】従来技術におけるファイアウォールの内部構成図である。
【図１４】パケットフィルタ装置の構成図。

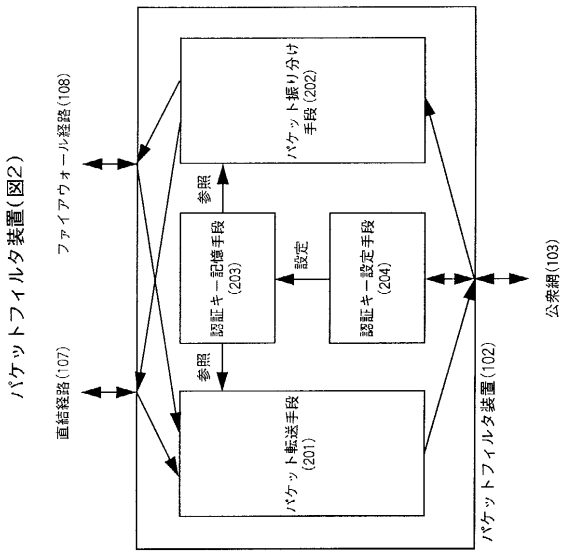
【符号の説明】

１０１…私設網、１０２…パケットフィルタ装置、１０３…公衆網、１０４…計算機、１０５…内部ルータ、１０６…ファイアウォール、１０７…直結経路、１０８…ファイアウォール経路、２０１…パケット転送手段、２０２…パケット振り分け手段、２０３…認証キー記憶手段、２０４…認証キー設定手段、３０１…経路判定手段、３０２…認証情報作成手段、３０３…認証情報付加手段、４０１…パケット判定手段、４０２…認証情報検査手段、４０３…認証情報削除手段、５０１…送信先アドレス、５０２…送信元アドレス、５０３…ポート番号、５０４…制御データ、５０５…制御ヘッダ、５０６…認証情報、５０７…データ、１００１…認証サーバ、１０１０…記憶手段、１０１１…パケットフィルタ装置認証手段、１０１２…認証キー送信手段、１３０１…入出力手段、１３０２…暗号化手段、１３０３…コネクション管理手段、１３０４…アプリケーション管理手段、１３０５…コネクション管理テーブルＡ、１３０６…コネクション管理テーブルＢ、１３０７…データパケット。

【図１】

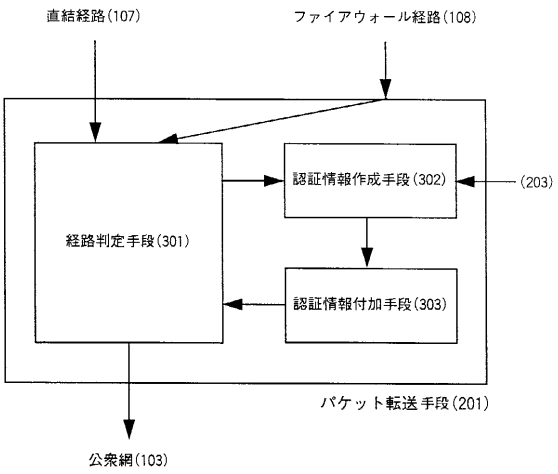


【図２】



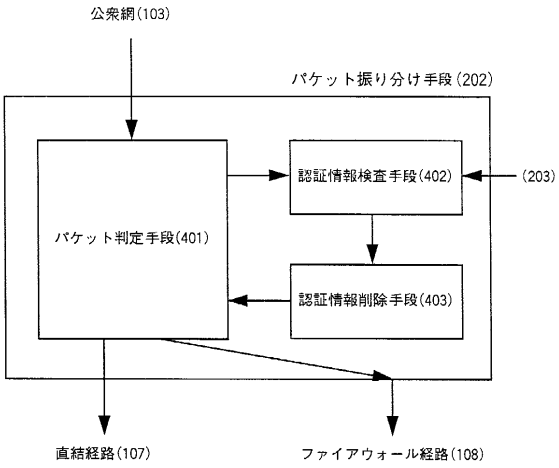
【図３】

パケット転送手段(図3)



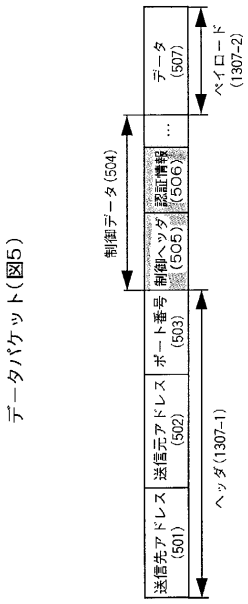
【図４】

パケット振り分け手段(図4)



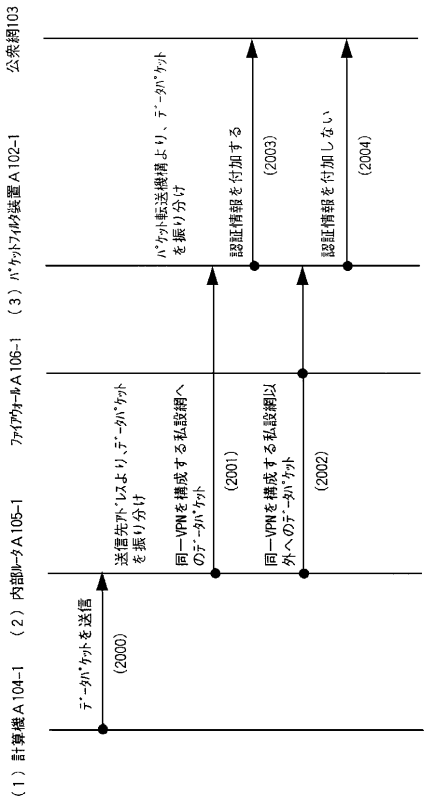
【図５】

データパケット(図5)



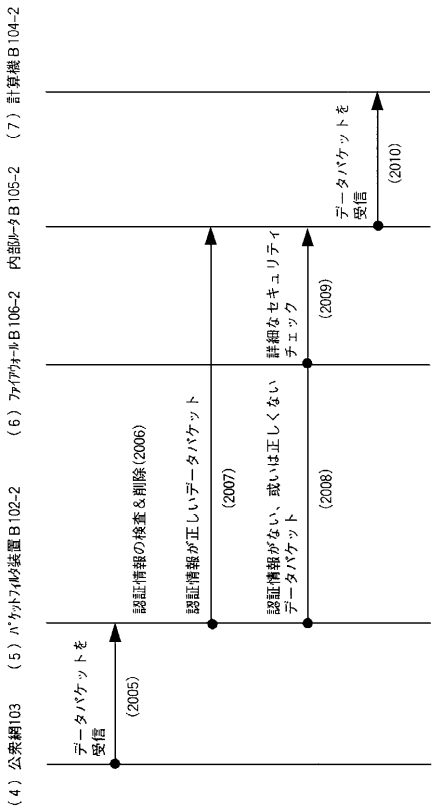
【図６】

処理の流れ(送信側)(図6)



【図７】

処理の流れ(受信側)(図7)



【図８】

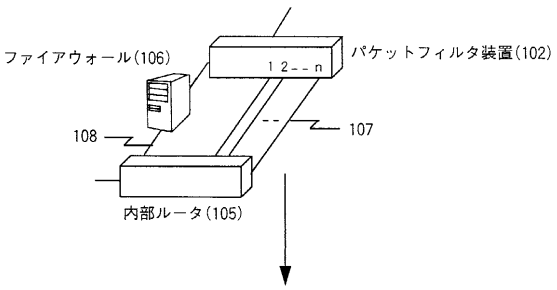
認証キー記憶手段の変更例1(図8)

認証キー記憶手段(203)

アドレス情報	認証キー情報
VPNグループAの宛先アドレス群	認証キーA
VPNグループBの宛先アドレス群	認証キーB
VPNグループCの宛先アドレス群	認証キーC
----	----

【図９】

認証キー記憶手段の変形例2(図9)

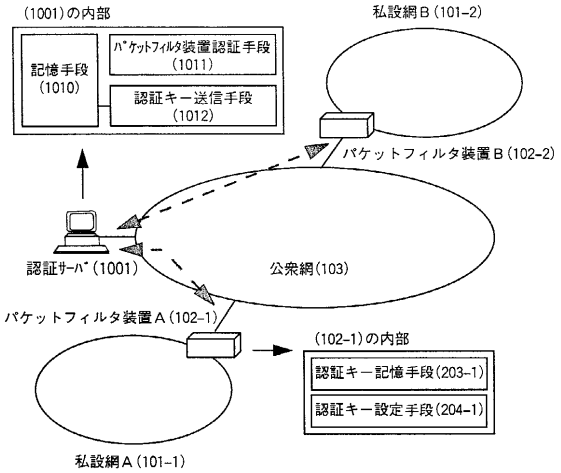


認証キー記憶手段(203)

直結経路番号	認証キー情報
1	認証キー1
2	認証キー2
----	----
n	認証キーn

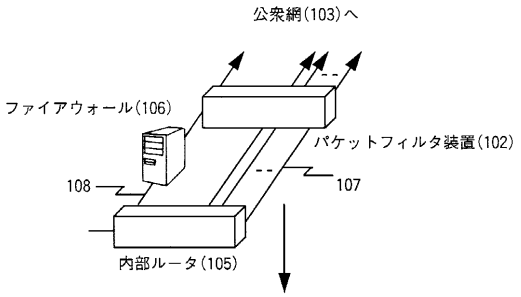
【図１０】

認証サーバ(図10)



【図１１】

パケットフィルタ装置の変形例(図11)

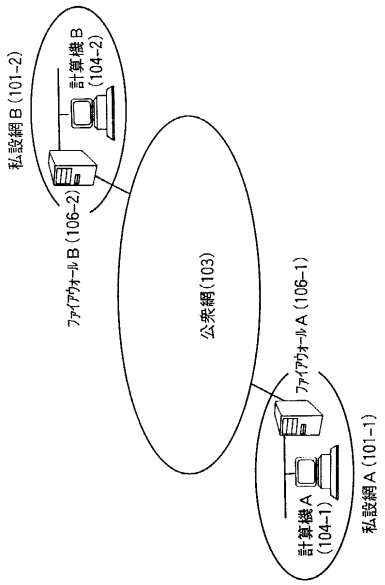


認証キー記憶手段(203)

直結経路番号	認証キー情報
1	認証キー１
2	認証キー２
⋮	⋮
n	認証キーｎ

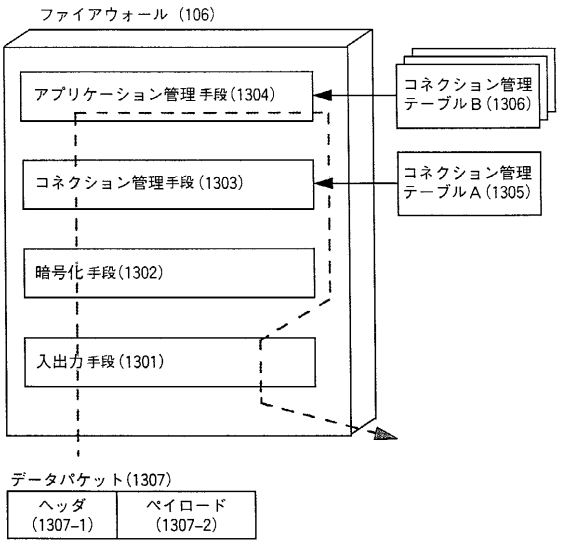
【図１２】

従来技術(図12)



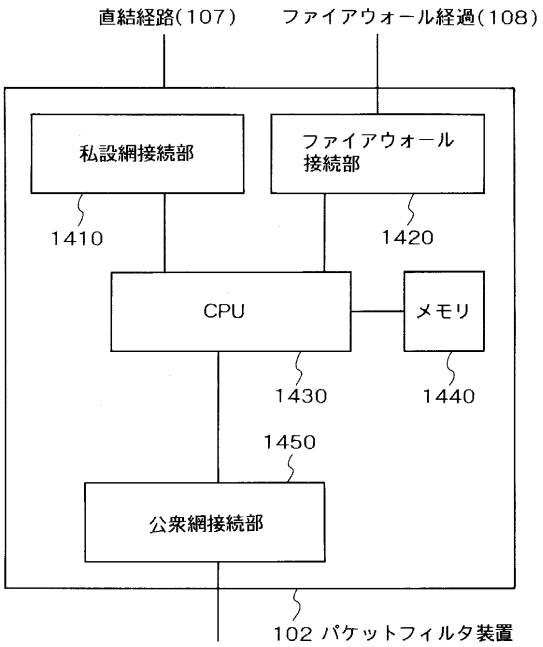
【図１３】

ファイアウォールの内部構成(図13)



【図１４】

図14



フロントページの続き

(72)発明者　川口　研治
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
(72)発明者　太田　正孝
神奈川県横浜市戸塚区戸塚町２１６番地　株式会社日立製作所　情報通信事業部内

審査官　石井　研一

(56)参考文献　特開平０９－２７０８２０（ＪＰ，Ａ）
特開平０９－２３３１１０（ＪＰ，Ａ）
特開平０８－３３１１５９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 12/66
H04L 9/32
H04L 12/56