(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3723896号
(P3723896)
(45)発行日　平成17年12月7日(2005.12.7)　(24)登録日　平成17年9月30日(2005.9.30)

(51)Int.Cl.[7]	F I		
H04L 12/22	H04L	12/22	
H04L 12/46	H04L	12/46	V
H04L 12/56	H04L	12/56	H
H04L 12/66	H04L	12/66	B

請求項の数 14　(全 13 頁)

(21)出願番号　特願2001-121508(P2001-121508)
(22)出願日　平成13年4月19日(2001.4.19)
(65)公開番号　特開2002-319938(P2002-319938A)
(43)公開日　平成14年10月31日(2002.10.31)
審査請求日　平成15年10月15日(2003.10.15)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100077274
弁理士　磯村　雅俊
(74)代理人　100102587
弁理士　渡邊　昌幸
(72)発明者　村山　純一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　原　博之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　清水　稔

最終頁に続く

(54)【発明の名称】パケット通信ネットワークシステムとセキュリティ制御方法およびルーティング装置ならびにプログラムと記録媒体

(57)【特許請求の範囲】

【請求項１】

パケット通信を行うネットワークシステムであって、

パケットヘッダに当該パケットのセキュリティクラスを特定するクラス識別情報を付与する付与手段と、上記クラス識別情報に対応して当該パケットに対するセキュリティ制御を行う制御手段とを有し、

上記付与手段は、パケットの送信元を判別する手段と、予め上記パケットの送信元別に上記クラス識別情報を対応付けた登録情報を記憶装置に記録する手段とを有し、上記パケットヘッダに付与するクラス識別情報を、当該パケットの送信元の判別結果に基づき上記登録情報を参照して特定することを特徴とするパケット通信ネットワークシステム。

【請求項２】

パケット通信を行うネットワークシステムであって、

パケットヘッダに当該パケットのセキュリティクラスを特定するクラス識別情報を付与する付与手段と、上記クラス識別情報に対応して当該パケットに対するセキュリティ制御を行う制御手段とを有し、

上記付与手段は、パケットの送信元のネットワークを判別する手段と、予め上記アクセスリンク毎に上記クラス識別情報を対応付けた登録情報を記憶装置に記録する手段とを有し、上記パケットヘッダに付与するクラス識別情報を、当該パケットの送信元のアクセスリンクの判別結果に基づき上記登録情報を参照して特定することを特徴とするパケット通信ネットワークシステム。

【請求項３】
請求項１または２に記載のパケット通信ネットワークシステムであって、
上記制御手段は、予め上記クラス識別情報別に上記パケットの送信先を対応付けた登録情報を記憶装置に記録する手段を有し、上記パケットヘッダに付与された上記クラス識別情報を判別し、判別したクラス識別情報に対応するパケットの送信先を上記登録情報を参照して特定し、特定した送信先に当該パケットを送出することを特徴とするパケット通信ネットワークシステム。
【請求項４】
請求項１または２に記載のパケット通信ネットワークシステムであって、
上記制御手段は、予め上記クラス識別情報別に上記パケットの送出先ネットワークを対応付けた登録情報を記憶装置に記録する手段を有し、上記パケットヘッダに付与された上記クラス識別情報を判別し、判別したクラス識別情報に対応するパケットの送出先ネットワークを上記登録情報を参照して特定し、特定した送出先ネットワークに当該パケットを送出することを特徴とするパケット通信ネットワークシステム。
【請求項５】
複数のパケット通信ネットワーク間を接続してパケットの中継通信を行うネットワークシステムであって、
中継元のネットワークから入力されたパケットに中継用パケットヘッダを付与してカプセル化すると共に、該中継用パケットヘッダに当該中継パケットのセキュリティクラスを特定するクラス識別情報を付与する付与手段と、上記クラス識別情報に基づき当該中継パケットに対するセキュリティ制御を行う制御手段とを有することを特徴とするパケット通信ネットワークシステム。
【請求項６】
請求項５に記載のパケット通信ネットワークシステムであって、
上記付与手段は、パケットの入力元のアクセスリンクあるいは仮想ＬＡＮを判別する手段と、予め上記アクセスリンクあるいは仮想ＬＡＮ毎に上記クラス識別情報を対応付けた登録情報を記憶装置に記録する手段とを有し、上記中継用パケットヘッダに付与するクラス識別情報を、当該パケットの入力元のアクセスリンクあるいは仮想ＬＡＮの判別結果に基づき上記登録情報を参照して特定することを特徴とするパケット通信ネットワークシステム。
【請求項７】
請求項５、もしくは、請求項６のいずれかに記載のパケット通信ネットワークシステムであって、
上記制御手段は、予め上記クラス識別情報別に上記中継パケットの送出先ネットワークのアクセスリンクあるいは仮想ＬＡＮを対応付けた登録情報を記憶装置に記録する手段を有し、上記中継用パケットヘッダに付与された上記クラス識別情報を判別し、判別したクラス識別情報に対応する送出先ネットワークのアクセスリンクあるいは仮想ＬＡＮを上記登録情報を参照して特定し、特定したアクセスリンクあるいは仮想ＬＡＮに当該中継パケットを送出することを特徴とするパケット通信ネットワークシステム。
【請求項８】
請求項７に記載のパケット通信ネットワークシステムであって、
上記制御手段は、上記判別したクラス識別情報に対応する送出先ネットワークのアクセスリンクあるいは仮想ＬＡＮが上記登録情報に無ければ、当該中継パケットを廃棄することを特徴とするパケット通信ネットワークシステム。
【請求項９】
外部のパケット通信ネットワークに接続される複数のエッジノードと各エッジノード間を接続する中継ノードからなり、複数の外部パケット通信ネットワーク間をエッジノードを介して接続し、各々の外部パケット通信ネットワークに対応して予め設定されたアクセスリンクあるいは仮想ＬＡＮ情報に基づき、各外部パケット通信ネットワーク間でのパケットの中継転送を行うネットワークシステムであって、

発側のエッジノードの機能として、中継元の外部パケット通信ネットワークのアクセスリンクあるいは仮想ＬＡＮから入力されたパケットに中継用パケットヘッダを付与してカプセル化する機能と、該中継用パケットヘッダに、予め当該アクセスリンクあるいは仮想ＬＡＮに対してテーブル設定されたセキュリティクラスの識別情報を読み出して付与する機能とを設け、
着側のエッジノードの機能として、中継用パケットヘッダに付与された上記識別情報を判別する機能と、判別した識別情報に対応して予めテーブル設定された中継先の外部パケット通信ネットワークのアクセスリンクあるいは仮想ＬＡＮ情報を読み出して当該アクセスリンクあるいは仮想ＬＡＮを特定する機能と、特定したアクセスリンクあるいは仮想ＬＡＮに当該パケットを送出する機能とを設けることを特徴とするパケット通信ネットワークシステム。

【請求項１０】

請求項９に記載のパケット通信ネットワークシステムであって、
上記着側のエッジノードの機能として、上記判別した識別情報に対応する上記中継先のネットワークのアクセスリンク情報がテーブル設定されていなければ、当該パケットを廃棄する機能を有することを特徴とするパケット通信ネットワークシステム。

【請求項１１】

請求項１から請求項８のいずれかに記載のパケット通信ネットワークシステムに設けられ、予め登録された転送テーブルに基づきパケットのルーティング処理を行う機能と、請求項１から請求項８のいずれかに記載の各機能とを有することを特徴とするルーティング装置。

【請求項１２】

コンピュータに請求項１１に記載のルーティング装置が有する各機能を実現させるためのプログラム。

【請求項１３】

コンピュータに請求項１１に記載のルーティング装置が有する各機能を実現させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項１４】

外部のパケット通信ネットワークに接続される複数のエッジノードと各エッジノード間を接続する中継ノードからなり、複数の外部パケット通信ネットワーク間をエッジノードを介して接続し、各々の外部パケット通信ネットワークに対応して予め設定されたアクセスリンクあるいは仮想ＬＡＮ情報に基づき、各外部パケット通信ネットワーク間でのパケットの中継転送を行うネットワークにおけるパケットに対するセキュリティ制御方法であって、
中継元の外部パケット通信ネットワークのアクセスリンクあるいは仮想ＬＡＮから入力されたパケットに中継用パケットヘッダを付与してカプセル化するステップと、
該中継用パケットヘッダに、予め当該アクセスリンクあるいは仮想ＬＡＮに対してテーブル設定されたセキュリティクラスの識別情報を読み出して付与するステップと、
中継用パケットヘッダに上記識別情報を付与した中継用パケットをルーティング処理するステップと、
ルーティングした中継用パケットヘッダに付与された上記識別情報を判別するステップと、
判別した識別情報に対応して予めテーブル設定された中継先の外部パケット通信ネットワークのアクセスリンクあるいは仮想ＬＡＮ情報を読み出して当該アクセスリンクあるいは仮想ＬＡＮを特定するステップと、
特定したアクセスリンクあるいは仮想ＬＡＮに当該パケットを送出するステップと、
上記判別した識別情報に対応する上記中継先のネットワークのアクセスリンクあるいは仮想ＬＡＮ情報がテーブル設定されていなければ、当該パケットを廃棄するステップとを有することを特徴とするセキュリティ制御方法。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】
本発明は、ギガビットイーサネットを含むＬＡＮ（Local Area Network）やＡＴＭ（Asynchronous Transfer Mode）網などにおけるパケット通信技術に係わり、特に、セキュリティの強固な通信サービスを提供するのに好適なパケット通信ネットワークシステムとセキュリティ制御方法およびルーティング装置ならびにプログラムと記録媒体に関するものである。
【０００２】
【従来の技術】
従来のパケット通信を行うネットワークでは、セキュリティを強固にすることを目的として、着側のエッジノードにおいて、ユーザパケットの宛先アドレスや送信元アドレス、および、上位アプリケーションの情報等を検索キーとしてフィルタリング処理を行っていた。
【０００３】
このため、エッジノードが保有すべき転送テーブルには、宛先アドレスだけでなく送信元アドレスや上位アプリケーションの情報も検索キーとして記述する必要があった。このような技術はファイアウォールとして知られている。
【０００４】
しかし、このようなファイアウォール技術を用いたパケット通信ネットワークでは、フィルタリング処理に用いる転送テーブルが保有すべきテーブルエントリ数が、単なるパケット転送に用いる転送テーブルに比べて、著しく増加する。そのために、フィルタリング処理負荷が転送処理負荷に比べて重くなり、エッジノードが本来の転送性能を発揮できなくなるという問題があった。
【０００５】
また、中継専用ネットワークでパケットがどのようにフィルタリング処理されたかをユーザがリアルタイムに知ることも困難であるという問題があった。
【０００６】
【発明が解決しようとする課題】
解決しようとする問題点は、従来の技術では、パケット通信ネットワークのセキュリティを強固にするためのフィルタリング処理の負荷が重く、エッジノードでの転送性能が低下してしまう点である。
【０００７】
本発明の目的は、これら従来技術の課題を解決しパケット通信ネットワークの信頼性および性能を向上させることが可能なパケット通信ネットワークシステムとセキュリティ制御方法およびルーティング装置ならびにプログラムと記録媒体を提供することである。
【０００８】
【課題を解決するための手段】
上記目的を達成するため、本発明のパケット通信ネットワークシステムとセキュリティ制御方法およびルーティング装置は、パケット通信を行うネットワークにおいて、パケットヘッダに当該パケットのセキュリティクラスを特定する識別情報を付与し、この識別情報に基づき当該パケットに対するセキュリティ制御を行うことを特徴とする。例えば、複数のネットワーク（ユーザネットワーク）間を接続してパケットの中継処理を行う中継専用ネットワークにおいて、ＬＡＮ（Local Area Network）等の信頼性の高いユーザネットワークとのアクセスリンクからのパケットに対しては高いセキュリティクラスの識別情報を付与し、インターネット等の信頼性の低いユーザネットワークとのアクセスリンクからのパケットに対しては低いセキュリティクラスの識別情報を付与し、そして、このように低いセキュリティクラスの識別情報が付与されたパケットに関しては、高いセキュリティクラスのユーザネットワークへ送出されないように制御することを特徴とする。
【０００９】
【発明の実施の形態】

以下、本発明の実施の形態を、図面により詳細に説明する。
図１は、本発明に係るパケット通信ネットワークシステムを設けたパケット通信ネットワークの構成例を示すブロック図であり、図２は、図１のパケット通信ネットワークシステムにおけるパケットの構成例を示す説明図、図３は、図１のパケット通信ネットワークシステムにおけるエッジノードの発側機能の構成例を示すブロック図、図４は、図１のパケット通信ネットワークシステムにおけるエッジノードの着側機能の構成例を示すブロック図、そして、図５は、図１のパケット通信ネットワークシステムにおけるエッジノードのハードウェア構成例を示すブロック図である。

【００１０】

図５において、５１はＣＲＴ（Cathode Ray Tube）やＬＣＤ(Liquid Crystal Display)等からなる表示装置、５２はキーボードやマウス等からなる入力装置、５３はＨＤＤ（Hard Disk Drive）等からなる外部記憶装置、５４はＣＰＵ（Central Processing Unit）５４ａや主メモリ５４ｂおよび入出力インタフェース５４ｃ等を具備してコンピュータ処理を行なう情報処理装置、５５は本発明に係わるプログラムやデータを記録したＣＤ－ＲＯＭ（Compact Disc-Read Only Memory）もしくはＤＶＤ（Digital Video Disc/Digital Versatile Disc）等からなる光ディスク、５６は光ディスク５５に記録されたプログラムおよびデータを読み出すための駆動装置、５７はＬＡＮ（Local Area Network）カードやモデム等からなる通信装置である。

【００１１】

光ディスク５５に格納されたプログラムおよびデータを情報処理装置５４により駆動装置５６を介して外部記憶装置５３内にインストールした後、外部記憶装置５３から主メモリ５４ｂに読み込みＣＰＵ５４ａで処理することにより、情報処理装置５４内に、図３および図４に示す、本発明のルーティング装置としてのエッジノードの各機能が構成される。

【００１２】

図１におけるパケット通信ネットワークシステムは、３つのユーザパケット転送ネットワーク１Ｂ，１Ｃ，１Ｅと１つのインターネット１Ｄを中継専用パケット転送ネットワーク１Ａで接続した構成となっている。

【００１３】

ここで、ユーザパケット転送ネットワーク１Ｅにはサーバ１Ｑが接続され、また、ユーザパケット転送ネットワーク１Ｂにはクライアント１Ｋが接続され、ユーザパケット転送ネットワーク１Ｃにはクライアント１Ｍが接続され、そして、インターネット１Ｄにはクライアント１Ｏが接続されている。

【００１４】

また、中継専用パケット転送ネットワーク１Ａは、２つのエッジノード１Ｆ，１Ｇおよび１つのコアノード１Ｈで構成されており、コアノード１Ｈとエッジノード１Ｆはコアリンク１Ｉで接続されており、コアノード１Ｈとエッジノード１Ｇはコアリンク１Ｊで接続されている。

【００１５】

さらに、ユーザパケット転送ネットワーク１Ｂ内のクライアント１Ｋは、中継専用パケット転送ネットワーク１Ａのエッジノード１Ｆとアクセスリンク１Ｌで接続されており、ユーザパケット転送ネットワーク１Ｃ内のクライアント１Ｍは、中継専用パケット転送ネットワーク１Ａのエッジノード１Ｆとアクセスリンク１Ｎで接続されており、インターネット１Ｄ内のクライアント１Ｏは、中継専用パケット転送ネットワーク１Ａのエッジノード１Ｆとアクセスリンク１Ｐで接続されており、ユーザパケット転送ネットワーク１Ｅ内のサーバ１Ｑは、中継専用パケット転送ネットワーク１Ａのエッジノード１Ｇと２本のアクセスリンク１Ｒ，１Ｓで接続されている。

【００１６】

各リンクの識別子として、コアリンク１ＩにはＬｉｎｋ＃Ａが割り当てられ、同様に、コアリンク１ＪにはＬｉｎｋ＃Ｂが、アクセスリンク１ＬにはＬｉｎｋ＃１が、アクセスリンク１ＮにはＬｉｎｋ＃２が、アクセスリンク１ＰにはＬｉｎｋ＃３が、アクセスリンク

１ＲにはＬｉｎｋ＃４－１が、そして、アクセスリンク１ＳにはＬｉｎｋ＃４－２が割り当てられている。

【００１７】

また、中継専用パケット転送ネットワーク１Ａのノード識別子（アドレス）として、エッジノード１ＦにはＣｏｒｅ＃Ａが、エッジノード１ＧにはＣｏｒｅ＃Ｂがそれぞれ割り当てられている。

【００１８】

さらに、ユーザパケット転送ネットワーク１Ｂ，１Ｃ，１Ｅおよびインターネット１Ｄのノード識別子（アドレス）として、クライアント１ＫにはＩＰ＃１が、クライアント１ＭにはＩＰ＃２が、クライアント１ＯにはＩＰ＃３が、サーバ１ＱにはＩＰ＃４がそれぞれ割り当てられている。

【００１９】

以上の各ネットワークのリンクの設定や識別子の割り当てなどは、後の図２の説明において述べる「セキュリティクラス」と共に、各ユーザ（ユーザパケット転送ネットワーク１Ｂ，・・・）側との、中継専用パケット転送ネットワーク１Ａによる中継転送サービスの利用契約時等に決定される。

【００２０】

以下、このような構成のネットワークにおいて、各クライアント１Ｋ～１Ｏがサーバ１Ｑ宛にユーザパケットを送信する場合についてのセキュリティ処理について検討する。

【００２１】

この際、ユーザパケット転送ネットワーク１Ｂ，１Ｃおよびインターネット１Ｄから送信されるユーザパケットは、パケットフォーマット１Ｔに従った構成になっている。このユーザパケットは、発側エッジノード１Ｆにおいて内部ＩＰヘッダが付加されてフォーマット変換され、中継専用パケット転送ネットワーク１Ａ内においては、内部ＩＰパケットが、パケットフォーマット１Ｕに従った構成になっている。

【００２２】

そして、この内部ＩＰパケットは、着側エッジノード１Ｇにおいて、内部ＩＰヘッダが除去されてフォーマット変換され、ユーザパケット転送ネットワーク１Ｅ内においては、ユーザパケットは、パケットフォーマット１Ｖに従った構成になっている。

【００２３】

中継専用パケット転送ネットワーク１Ａ内においては、内部パケットは、パケットフォーマット１Ｕに従った構成になっているが、内部ＩＰヘッダの部分は、具体的には図２に示すヘッダフォーマットのような構成である。

【００２４】

この図２に示すヘッダフォーマットは、ＩＥＴＦ（Internet Engineering Task Force）で規定されるＲＦＣ２４６０（Request For Comment２４６０）を修正した形になっており、ヘッダフォーマットのバージョンを示すＶｅｒｓｉｏｎフィールド２Ａ、内部ＩＰパケットの品質クラスを示すＴｒａｆｆｉｃ　Ｃｌａｓｓフィールド２Ｂ、内部ＩＰパケットのセキュリティクラスを示すＳｅｃｕｒｉｔｙ　Ｃｌａｓｓフィールド２Ｃ、内部ＩＰパケットのペイロードの長さを示すＰａｙｌｏａｄ　Ｌｅｎｇｈｔフィールド２Ｄ、内部ＩＰパケットのペイロード種別あるいはヘッダの拡張機能の種別を示すＮｅｘｔ　Ｈｅａｄｅｒフィールド２Ｅ、内部ＩＰパケットが許容する転送ホップ数を示すＨｏｐ　Ｌｉｍｉｔフィールド２Ｆ、内部ＩＰパケットの発側エッジノードを示すＳｏｕｒｃｅ　Ａｄｄｒｅｓｓフィールド２Ｇ、内部ＩＰパケットの着側エッジノードを示すＤｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓフィールド２Ｈで構成される。

【００２５】

ここで、ＲＦＣ２４６０と異なる点は、内部ＩＰパケットのセキュリティクラスを示すＳｅｃｕｒｉｔｙ　Ｃｌａｓｓフィールド２Ｃの部分であり、これが本実施例における重要なポイントとなっている。

【００２６】

なお、本例では，内部ＩＰパケットのヘッダ内にセキュリティクラスの識別情報を示すことがポイントであるため、必ずしも、図２に示すフォーマット例に限定してＳｅｃｕｒｉｔｙ　Ｃｌａｓｓフィールド２Ｃを定義しなければならないわけではない。

【００２７】

例えば、Ｓｅｃｕｒｉｔｙ　Ｃｌａｓｓフィールド２Ｃに割り当てている一部のフィールドのみを、セキュリティクラスを示すためのフィールドと定義しても良い。また、他のフィールドの一部、例えば、発側エッジノードを示すＳｏｕｒｃｅ　Ａｄｄｒｅｓｓフィールド２Ｇや着側エッジノードを示すＤｅｓｔｉｎａｔｉｏｎ　Ａｄｄｒｅｓｓフィールド２Ｈの一部をセキュリティクラスを示すためのフィールドと定義しても良い。

【００２８】

このような構成において、ユーザパケット転送ネットワーク１Ｂ，１Ｃおよびインターネット１Ｄから中継専用パケット転送ネットワーク１Ａへ転送されてくるユーザＩＰパケットを、発側エッジノード１Ｆにおいて内部ＩＰヘッダを付加してフォーマット変換するために、発側エッジノード１Ｆは、図３に示すような機能を装備する。

【００２９】

図３で示される発側エッジノード１Ｆは、セキュリティクラス識別部３Ａ、および、転送部３Ｂで構成され、また、装置外のノードと、アクセスリンク１Ｌ，１Ｎ，１Ｐおよびコアリンク１Ｉで接続されている。

【００３０】

アクセスリンク１Ｌ，１Ｎ，１Ｐから入力されたユーザＩＰパケットは、セキュリティクラス識別部３Ａに送られ、セキュリティクラス識別部３Ａは、セキュリティクラス識別テーブル３Ｃを保有しており、これを用いて、入力アクセスリンクからセキュリティクラスを特定する。すなわち、セキュリティクラス識別部３Ａは、送信元（本例ではアクセスリンク）を判別し、対応するセキュリティクラスを、セキュリティクラス識別テーブル３Ｃを参照して特定する。そして、セキュリティクラス識別部３Ａにおいて、セキュリティクラスが特定されたユーザＩＰパケットは、セキュリティクラス属性が付加され、転送部３Ｂへ送られる。

【００３１】

転送部３Ｂは、転送テーブル３Ｄを保有しており、これを用いて、ユーザパケットの宛先ユーザＩＰアドレスから宛先内部ＩＰアドレスおよび出力コアリンクを特定する。また、この情報を基に、内部ＩＰヘッダを生成し、これに先に特定したセキュリティクラス属性等も記述した後、ユーザＩＰパケットに付加して内部パケットを生成する。そして、このように、生成した内部パケットを、特定された出力コアリンクから出力する。

【００３２】

一方、中継専用パケット転送ネットワーク１Ａから、ユーザパケット転送ネットワーク１Ｅへ転送されてくる内部ＩＰパケットに対して、着側エッジノード１Ｇにおいて、内部ＩＰヘッダを除去してフォーマット変換するために、着側エッジノード１Ｇは、図４に示すような機能を有する。

【００３３】

図４に示すように、着側エッジノード１Ｇは、転送部４Ｂ、および、セキュリティクラス識別部４Ａで構成され、また、着側エッジノード１Ｇは、装置外のノードと、コアリンク１Ｊおよびアクセスリンク１Ｒ，１Ｓで接続されている。

【００３４】

コアリンク１Ｊから入力されたユーザＩＰパケットは転送部４Ｂに送られる。転送部４Ｂは、転送テーブル４Ｄを保有しており、これを用いて、ユーザＩＰパケットの宛先ユーザＩＰアドレスから出力アクセスリンクのグループを特定する。そして、出力アクセスリンクのグループを識別したユーザＩＰパケットを、セキュリティクラス属性とともに、セキュリティクラス識別部４Ａへ送出する。

【００３５】

転送部４Ｂからのユーザ ＩＰパケットを受信したセキュリティクラス識別部４Ａは、セキ

ュリティクラス識別テーブル４Ｃを保有しており、これを用いて、セキュリティクラスから出力アクセスリンクを特定する。この場合、テーブルエントリの内容によっては、出力アクセスリンクを特定するのではなく、パケット廃棄を指示する場合もある。

【００３６】

以上のようにして、本例のパケット通信ネットワークシステムでは、発側エッジノード１Ｆにおいて、セキュリティ識別テーブル３Ｃにより、各ユーザパケット転送ネットワークおよびインターネットのセキュリティクラスを決定する。本例では、ユーザパケット転送ネットワーク１Ｂがセキュリティクラス＃１に、ユーザパケット転送ネットワーク１Ｃがセキュリティクラス＃２に、そして、インターネット１Ｄがセキュリティクラス＃３に、それぞれ割り当てられている。

【００３７】

また、着側エッジノード１Ｇにおいて、セキュリティクラス識別部４Ａにより、セキュリティ識別テーブル４Ｃに基づき、実行すべきセキュリティ処理をセキュリティクラス毎に決定する。本例では、セキュリティクラス＃１のユーザパケットをアクセスリンクＬｉｎｋ＃４－１へ、また、セキュリティクラス＃２のユーザパケットをアクセスリンクＬｉｎｋ＃４－２へそれぞれ出力するように規定されており、そして、セキュリティクラス＃３のユーザパケットは廃棄するように規定されている。

【００３８】

これにより、サーバ１Ｑへの、不特定のユーザを収容するインターネットからのアクセスを遮断するといったことが可能となる。

【００３９】

また、特定のユーザパケット転送ネットワークについても、ネットワーク毎にセキュリティがクラス分けされているために、信頼性の高いセキュリティクラス＃１のユーザＩＰパケットについては、サーバ１Ｑにおいて認証処理を行うことなくサービスを提供し、また、信頼性が中程度のセキュリティクラス＃２のユーザＩＰパケットについては、サーバ１Ｑにおいて認証処理を行った結果でサービス提供の有無を判断するといったことが可能となる。

【００４０】

この結果、セキュリティ処理を高速に行うだけでなく、ユーザ毎に、異なるセキュリティサービスを提供するといったことが可能となり、本例によれば、エンドユーザ間での転送性能を劣化させることなく、強固なセキュリティ処理を施すことが可能となる。

【００４１】

また、エンドユーザ自身が、受信アクセスリンクを使い分けて、各受信パケット毎に適切なセキュリティ処理を施すことで、ユーザ毎に、異なるセキュリティサービスを提供するといったことが可能となる。

【００４２】

図６は、図１におけるパケット通信ネットワークシステムの本発明に係わる処理動作例を示すフローチャートである。

【００４３】

図１における中継専用パケット転送ネットワーク１Ａでは、発側のエッジノード１Ｆにおいて、中継元のネットワーク（１Ｂ，１Ｃ，１Ｄ）のアクセスリンク（１Ｌ，１Ｎ，１Ｐ）から入力されたパケット（１Ｔ）に中継用パケットヘッダ（内部ＩＰヘッダ）を付与してカプセル化する（ステップ６０１）と共に、この中継用パケットヘッダに、予め当該アクセスリンク（１Ｌ，１Ｎ，１Ｐ）に対してテーブル（図３におけるセキュリティクラス識別テーブル３Ｃ）に設定されたセキュリティクラスの識別情報（ＳＣ＃１，ＳＣ＃２，ＳＣ＃３，・・・）を読み出して付与する（ステップ６０２）。

【００４４】

そして、中継用パケットヘッダに識別情報を付与した中継用パケットを、コアリンク１Ｉ、コアノード１Ｈ、コアリンク１Ｊを介して、着側のエッジノード１Ｇまでルーティング処理する（ステップ６０３）。

【００４５】
着側のエッジノード１Ｇでは、ルーティングされてきた中継用パケットヘッダ（内部ＩＰヘッダ）に付与された識別情報（ＳＣ＃１，ＳＣ＃２，ＳＣ＃３，・・・）を判別し（ステップ６０４）、判別した識別情報に対応して予めテーブル（図４におけるセキュリティクラス識別テーブル４Ｃ）に設定された中継先のネットワークのアクセスリンク情報（Ｌｉｎｋ＃４－１，Ｌｉｎｋ＃４－２，・・・）を読み出し（ステップ６０５）、当該アクセスリンクを特定できれば（ステップ６０６）、特定したアクセスリンクに当該パケットを送出する（ステップ６０７）。
【００４６】
また、図４におけるセキュリティクラス識別テーブル４Ｃにおいて、セキュリティクラスＳＣ＃３に対して「廃棄」として対応付けられているように、ステップ６０６において、判別した識別情報に対応する中継先のネットワークのアクセスリンク情報がテーブル設定されていなければ、当該パケットを廃棄する（ステップ６０８）。
【００４７】
以上、図１～図６を用いて説明したように、本例のパケット通信ネットワークシステムとセキュリティ制御方法では、ユーザデータをカプセル化するために使用されるパケットヘッダにセキュリティクラスの識別情報を記述し、さらに、複数のユーザネットワーク間を中継する専用のパケット転送ネットワークとして構成し、各ユーザネットワーク間において、ユーザパケットを中継専用パケットにカプセル化して転送する。
【００４８】
そして、この中継転送する際、ユーザネットワークと中継専用パケット転送ネットワークを接続するエッジノード（ルーティング装置）において、ユーザネットワークから中継専用パケット転送ネットワークへのユーザパケットの入力時には、ユーザネットワークを収容するアクセスリンクに応じて、中継専用パケットのセキュリティクラスを決定し、中継専用パケットのヘッダに付与して中継専用パケット転送ネットワーク内で転送すると共に、中継専用パケット転送ネットワークからユーザネットワークへの出力時には、中継専用パケットのセキュリティクラスに応じて、ユーザネットワークを収容するアクセスリンクを決定して出力、あるいは該当する中継専用パケットを廃棄する。
【００４９】
このように、本例では、パケット通信ネットワークにおいて、ユーザデータをカプセル化するために使用するパケットヘッダにセキュリティクラスの識別情報を記述することで、宛先アドレス、送信元アドレス、上位アプリケーションの情報等の多数の情報をセキュリティクラスに集約させることが可能となり、フィルタリング処理を、このセキュリティクラスを基に行うことで、転送性能の劣化を最小限に抑制することが可能となる。
【００５０】
さらに、パケット通信ネットワークを、ユーザネットワーク間の中継専用パケット転送ネットワークとし、ユーザネットワーク間においては、ユーザパケットを中継専用パケットにカプセル化して転送するので、セキュリティクラスをユーザが勝手に記述することを不可能とさせ、セキュリティを強固なものにすることが可能となる。
【００５１】
また、各ユーザネットワーク側との間で、中継転送サービスの契約時等において、各ユーザネットワークに割り当てるアクセスリンク毎にセキュリティクラスを決定してテーブル設定しておき、このテーブル内容に基づき、発側のエッジノードにおいて、ユーザネットワークを収容するアクセスリンクに応じて、中継専用パケットのセキュリティクラスを決定することで、ユーザパケットの宛先アドレス、送信元アドレス、上位アプリケーションの情報等を検索キーとして参照することなく、セキュリティクラスを決定することができる。ここで、アクセスリンク数は、宛先アドレス、送信元アドレス、上位アプリケーションの情報等の組み合わせ数よりも少ないために、発側エッジノードにおける転送処理をほとんど劣化させないで済む。
【００５２】

さらに、着側のエッジノードにおいて、中継専用パケットのセキュリティクラスに応じて、ユーザネットワークを収容するアクセスリンクを決定する、あるいは該当する中継専用パケットを廃棄することで、セキュリティクラスを検索キーとして参照するだけで、フィルタリング処理を行うことができる。このセキュリティクラスは、通常は数クラスしか設けないために、転送処理をほとんど劣化させないで済む。

【００５３】

この結果、エンドユーザ間での転送性能を劣化させることなく、強固なセキュリティ処理を施すことが可能となる。また、エンドユーザは、受信するアクセスリンク毎に、受信パケットのセキュリティクラスを認識することが可能となり、それぞれのアクセスリンク毎に、適切なセキュリティ処理をユーザ自身が施すことが可能となる。

【００５４】

尚、本発明は、図１～図６を用いて説明した例に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能である。例えば、本例では、複数のユーザネットワーク間を接続してユーザパケットを中継転送する専用のパケット通信ネットワーク（中継専用パケット転送ネットワーク１Ａ）に、本発明に係わるセキュリティ制御を行うルーティング装置（エッジノード１Ｆ，１Ｇ）を設け、中継専用パケットにカプセル化する際に、セキュリティクラスのヘッダ付与を行う構成としているが、各ユーザネットワーク内に設けられたそれぞれのルータにおいて同様のセキュリティ制御を行う等することにより、他のネットワーク構成においても本発明を適用することができる。この場合、セキュリティクラスは、図１に示すパケットフォーマット１Ｔ，１Ｖにおけるユーザ ＩＰヘッダに記述される。

【００５５】

また、本例では、インターネット１Ｄを有するネットワーク、すなわち、ＩＰパケットを例としているが、同じくＩＰパケットを用いるイントラネット（この場合、セキュリティクラスは高く設定される）を接続することもでき、また、セルを用いるＡＴＭ（Asynchronous Transfer Mode）ネットワークなどにも、セルヘッダにセキュリティクラスを付与する等して適用することが可能である。尚、本例におけるパケットの送信元のネットワークの識別に用いるアクセスリンクは、ＡＴＭにおけるＶＰ／ＶＣであり、また、ギガビットイーサネット（ＩＥＥＥ８０２．１Ｑ）における仮想ＬＡＮ（ＶＬＡＮ－ＩＤ）である。

【００５６】

また、本例では、ルーティング機能を有するエッジノードの構成として図５のコンピュータ構成例を示したが、キーボードや光ディスクの駆動装置の無いコンピュータ構成としても良い。また、本例では、光ディスクを記録媒体として用いているが、ＦＤ（Flexible Disk）等を記録媒体として用いることでも良い。また、プログラムのインストールに関しても、通信装置を介してネットワーク経由でプログラムをダウンロードしてインストールすることでも良い。

【００５７】

【発明の効果】

本発明によれば、パケット通信ネットワークのセキュリティを強固にするためのフィルタリング処理の負荷を軽減でき、エッジノードでの転送性能の低下を回避でき、パケット通信ネットワークの信頼性および性能を向上させることが可能である。

【図面の簡単な説明】

【図１】本発明に係るパケット通信ネットワークシステムを設けたパケット通信ネットワークの構成例を示すブロック図である。

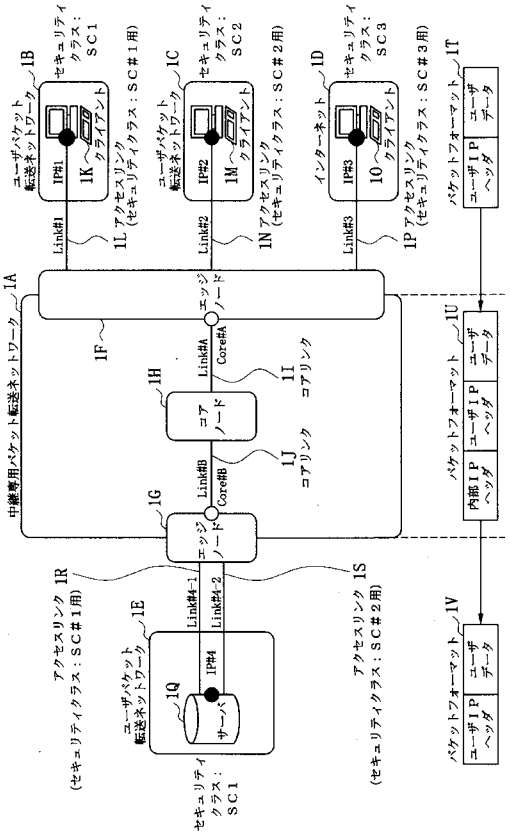
【図２】図１のパケット通信ネットワークシステムにおけるパケットの構成例を示す説明図である。

【図３】図１のパケット通信ネットワークシステムにおけるエッジノードの発側機能の構成例を示すブロック図である。

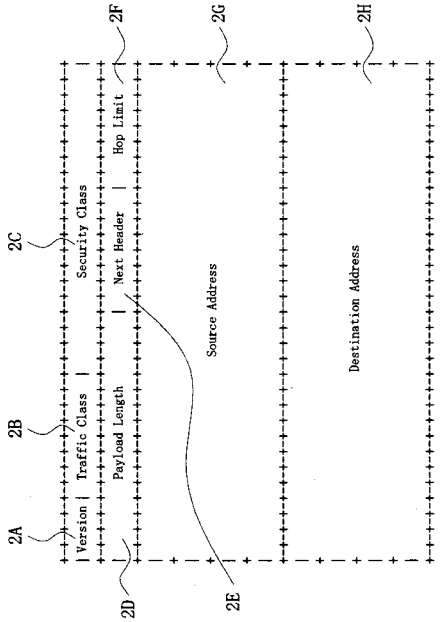
【図４】図１のパケット通信ネットワークシステムにおけるエッジノードの着側機能の構成例を示すブロック図である。

【図５】図１のパケット通信ネットワークシステムにおけるエッジノードのハードウェア構成例を示すブロック図である。
【図６】図１におけるパケット通信ネットワークシステムの本発明に係わる処理動作例を示すフローチャートである。
【符号の説明】
１Ａ：中継専用パケット転送ネットワーク、１Ｂ，１Ｃ，１Ｅ：ユーザパケット転送ネットワーク、１Ｄ：インターネット、１Ｆ：エッジノード（発側）、１Ｇ：エッジノード（着側）、１Ｈ：コアノード、１Ｉ，１Ｊ：コアリンク、ｉＫ，１Ｍ，１Ｏ：クライアント、１Ｌ，１Ｎ，１Ｐ，１Ｒ，１Ｓ：アクセスリンク、１Ｑ：サーバ、１Ｔ，１Ｕ，１Ｖ：パケットフオーマット、２Ａ：Ｖｅｒｓｉｏｎフィールド、２Ｂ：Ｔｒａｆｆｉｃ Ｃｌａｓｓフィールド、２Ｃ：Ｓｅｃｕｒｉｔｙ Ｃｌａｓｓフィールド、２Ｄ：Ｐａｙｌｏａｄ Ｌｅｎｇｈｔフィールド、２Ｅ：Ｎｅｘｔ Ｈｅａｄｅｒフィールド、２Ｆ：Ｈｏｐ Ｌｉｍｉｔフィールド、２Ｇ：Ｓｏｕｒｃｅ Ａｄｄｒｅｓｓフィールド、２Ｈ：Ｄｅｓｔｉｎａｔｉｏｎ Ａｄｄｒｅｓｓフィールド、３Ａ：セキュリティクラス識別部、３Ｂ：転送部、セキュリティクラス識別テーブル、３Ｄ：転送テーブル、４Ａ：セキュリティクラス識別部、４Ｂ：転送部、４Ｃ：セキュリティクラス識別テーブル、４Ｄ：転送テーブル、５１：表示装置、５２：入力装置、５３：外部記憶装置、５４：情報処理装置、５４ａ：ＣＰＵ、５４ｂ：主メモリ、５４ｃ：入出力インタフェース、５５：光ディスク、５６：駆動装置、５７：通信装置。

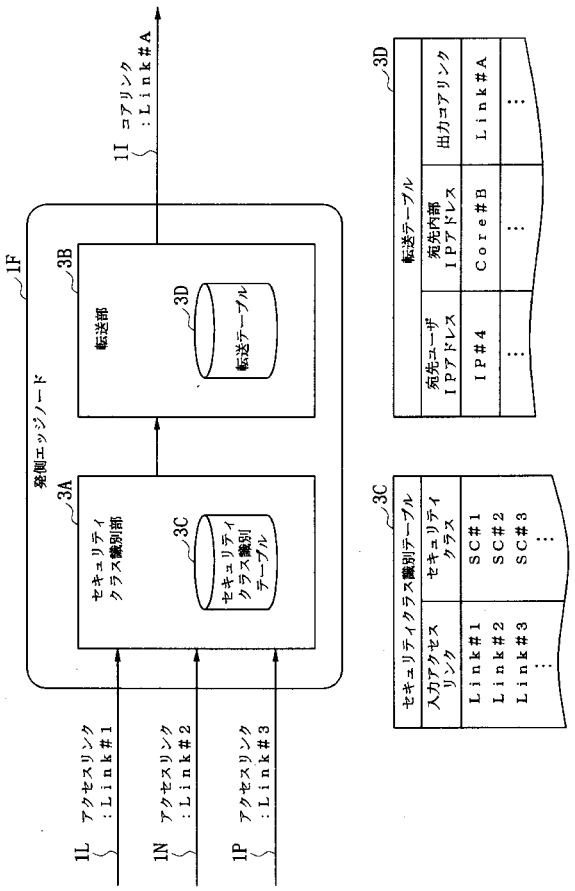
【図１】



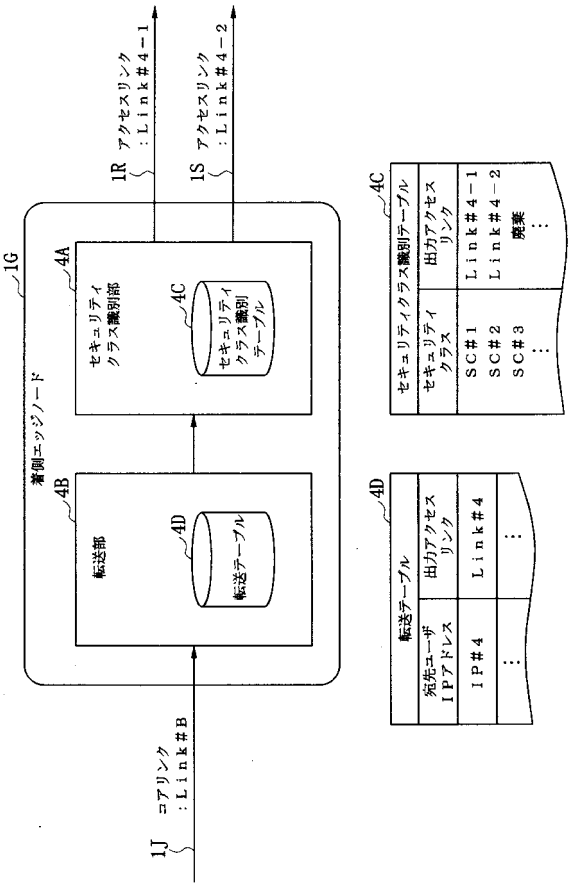
【図２】



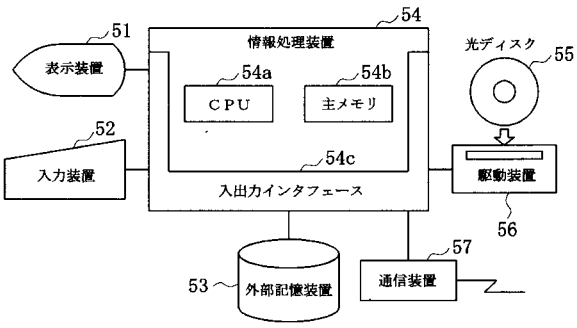
【図３】


1I コアリンク :Link#A
1F
発側エッジノード
3B
転送部
3D
転送テーブル
3A
セキュリティクラス識別部
3C
セキュリティクラス識別テーブル
1L アクセスリンク :Link#1
1N アクセスリンク :Link#2
1P アクセスリンク :Link#3
3D
転送テーブル
宛先ユーザIPアドレス
宛先内部IPアドレス
出力コアリンク
IP#4
Core#B
Link#A
3C
セキュリティクラス識別テーブル
入力アクセスリンク
セキュリティクラス
Link#1 SC#1
Link#2 SC#2
Link#3 SC#3

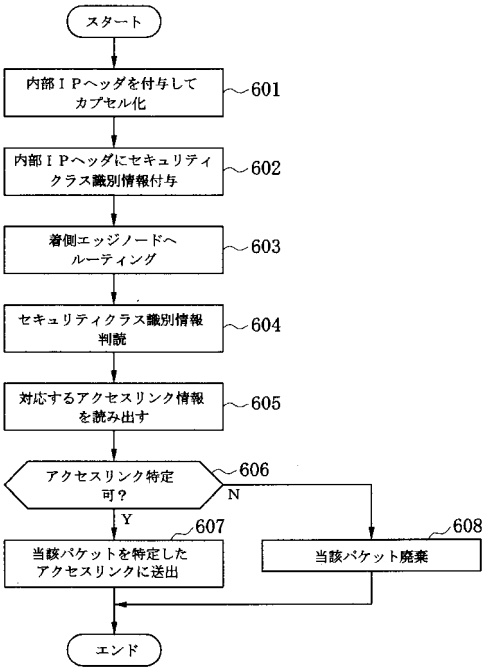
【図４】


1R アクセスリンク :Link#4-1
1S アクセスリンク :Link#4-2
1G
着側エッジノード
4A
セキュリティクラス識別部
4C
セキュリティクラス識別テーブル
4B
転送部
4D
転送テーブル
1J コアリンク :Link#B
4C
セキュリティクラス識別テーブル
セキュリティクラス
出力アクセスリンク
SC#1 Link#4-1
SC#2 Link#4-2
SC#3 廃棄
4D
転送テーブル
宛先ユーザIPアドレス
出力アクセスリンク
IP#4 Link#4

【図５】


51
表示装置
54
情報処理装置
54a
CPU
54b
主メモリ
光ディスク
55
52
入力装置
54c
入出力インタフェース
駆動装置
56
53
外部記憶装置
57
通信装置

【図６】


スタート
内部ＩＰヘッダを付与してカプセル化
601
内部ＩＰヘッダにセキュリティクラス識別情報付与
602
着側エッジノードへルーティング
603
セキュリティクラス識別情報判読
604
対応するアクセスリンク情報を読み出す
605
アクセスリンク特定可？
606
N
Y
当該パケットを特定したアクセスリンクに送出
607
当該パケット廃棄
608
エンド

フロントページの続き

(56)参考文献 特開平０８－１０２７４５（ＪＰ，Ａ）
特開平０５－２２７１６２（ＪＰ，Ａ）
特開平１１－２０５３８８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 12/22
H04L 12/46
H04L 12/56
H04L 12/66