(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-247858
(P2004-247858A)
(43)公開日　平成16年9月2日(2004.9.2)

(51)Int.Cl.[7]	F I			テーマコード（参考）
H04L 12/56	H04L	12/56	400A	5B085
G06F 15/00	G06F	15/00	310B	5K030

審査請求 未請求　請求項の数 8　ＯＬ　（全 27 頁）

(21)出願番号　特願2003-33940 (P2003-33940)
(22)出願日　平成15年2月12日 (2003.2.12)

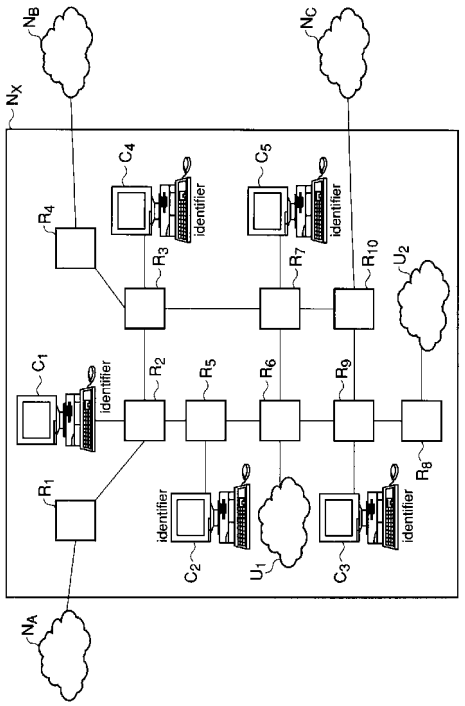
（特許庁注：以下のものは登録商標）
イーサネット

(71)出願人　503058267
淺野　正一郎
東京都世田谷区桜丘三丁目２０番２３号
(71)出願人　503058382
阿部　俊二
神奈川県横浜市青葉区千草台３７番地３９　２０３号室
(71)出願人　503058979
計　宇生
東京都練馬区田柄１丁目１８番２２号　３１２号室
(71)出願人　503058980
趙　偉平
神奈川県横浜市栄区小菅ヶ谷１丁目５番６号　２０１号室

最終頁に続く

(54)【発明の名称】情報提供システム及び情報提供方法

(57)【要約】
【課題】広域コンピュータネットワークを介しての外部からの不正目的のアクセスによるシステム被害を局所化することで、情報提供サービス全体の攻撃耐性の向上と稼働率の向上とを図ること。
【解決手段】本発明は、同一のネットワーク識別子が割り当てられており、広域ネットワーク上のユーザにサービスＳを提供するための複数のサーバ実体C_1乃至C_5と、広域ネットワーク上の一のネットワークから他のネットワークへの経路制御処理について定義した通常の経路制御処理テーブルと、上記所定のネットワーク識別子を送信先とする情報の経路制御処理について定義した経路制御処理テーブルとを有し、これらテーブルを参照して経路制御処理を行うことで、上記所定のサービスＳを提供する対象を所定単位で物理的に区分けするためのルータR_1乃至R_{10}と、を具備する情報提供システムである。
【選択図】　図１



【特許請求の範囲】
【請求項１】
広域ネットワーク上で稼動する情報提供システムにおいて、所定のネットワーク識別子が割り当てられており、上記広域ネットワーク上の対象に所定のサービスを提供するための複数の情報提供手段と、
上記広域ネットワーク上の一のネットワークから他のネットワークへの経路制御処理について定義した第１のテーブルと、上記所定のネットワーク識別子を送信先とする情報の経路制御処理について定義した第２のテーブルと、を少なくとも有しており、上記第１又は第２のテーブルのいずれかを参照して経路制御処理を行うことで、上記各情報提供手段が上記所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で物理的に区分けするための経路制御手段と、
を具備することを特徴とする情報提供システム。
【請求項２】
上記第２のテーブルは、上記所定のネットワーク識別子を送信先とする情報に対して、所定のラベルの付加、除去、変更をするラベル処理を行った後、所定の送信先に送信する旨、或いは、所定のラベルが付加された情報に対して、更なるラベル処理を行った後、所定の送信先に送信する旨、を少なくとも定義していることを更に特徴とする請求項１に記載の情報提供システム。
【請求項３】
上記所定のネットワーク識別子とはＩＰアドレスであり、
上記経路制御処理手段は、上記所定のネットワーク識別子を送信先とするＩＰパケットを受信したときには、上記第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて定められる更なるラベル処理を行った後、所定の送信先に送信する、
ことを更に特徴とする請求項２に記載の情報提供システム。
【請求項４】
広域ネットワーク上で稼動する情報提供システムにおいて、上記広域ネットワーク上の一のネットワークから他のネットワークへ送信すべきＩＰパケットを受信した場合には、第１のテーブルを参照して、当該ＩＰパケットを当該他のネットワークに送信し、一方、所定のサービスに係る所定のＩＰアドレスを送信先とするＩＰパケットを受信した場合には、第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて、当該ＩＰパケットに対して、所定のラベルの付加、除去、変更をするラベル処理を行った後に所定の送信先に送信する、エッジルータと、
上記ラベル処理がなされたＩＰパケットを受信した場合には、第３のテーブルを参照して、当該ＩＰパケットに含まれる所定のラベルに基づいて定められる更なるラベル処理を行った後に所定の送信先に送信する、コアルータと、
上記所定のサービスに係る所定のＩＰアドレスが割り当てられており、上記エッジルータ及びコアルータの少なくともいずれかを介してＩＰパケットを受信した場合には、当該ＩＰパケットに基づいた所定の情報を当該ＩＰパケットの送信元に送信する、複数のサーバ実体と、
を有し、上記エッジルータ及びコアルータによる経路制御処理により、上記サーバ実体により所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で物理的に区分けすることを特徴とする情報提供システム。
【請求項５】
広域ネットワーク上で稼動する情報提供システムによる情報提供方法において、
上記情報提供システムにより、
上記広域ネットワーク上の一のネットワークから他のネットワークへ送信すべき情報を受信した場合には、第１のテーブルを参照して、当該情報を当該他のネットワークに送信す

るよう経路制御処理を行い、
一方、所定のサービスに係る所定のネットワーク識別子を送信先とする情報を受信した場合には、第２のテーブルに基づく経路制御処理を行い、
上記経路制御処理により、上記所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で論理的に区分けする、
ことを特徴とする情報提供方法。
【請求項６】
上記第２のテーブルは、上記所定のネットワーク識別子を送信先とする情報に対して、所定のラベルの付加、除去、変更をするラベル処理を行った後、所定の送信先に送信する旨、或いは、所定のラベルが付加された情報に対して、更なるラベル処理を行った後、所定の送信先に送信する旨、を少なくとも定義していることを更に特徴とする請求項５に記載の情報提供方法。
【請求項７】
上記所定のネットワーク識別子とはＩＰアドレスであり、
上記情報提供システムにより、上記所定のネットワーク識別子を送信先とするＩＰパケットを受信したときには、上記第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて、当該ＩＰパケットに対して、所定のラベルの付加、除去、変更をするラベル処理を行った後、所定の送信先に送信することを更に特徴とする請求項６に記載の情報提供方法。
【請求項８】
エッジルータ、コアルータ、及びサーバ実体を有し、広域ネットワーク上で稼動する情報提供システムによる方法であって、
上記エッジルータにより、
上記広域ネットワーク上の一のネットワークから他のネットワークへ送信すべきＩＰパケットを受信した場合には、第１のテーブルを参照して、当該ＩＰパケットを当該他のネットワークに送信し、
一方、所定のサービスに係る所定のＩＰアドレスを送信先とするＩＰパケットを受信した場合には、第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて、当該ＩＰパケットに対して、所定のラベルの付加、除去、変更をするラベル処理を行った後に所定の送信先に送信し、
上記コアルータにより、
上記ラベル処理がなされたＩＰパケットを受信した場合には、第３のテーブルを参照して、当該ＩＰパケットに含まれる所定のラベルに基づいて定められる更なるラベル処理を行った後に所定の送信先に送信し、
上記サーバ実体により、
上記エッジルータ及びコアルータの少なくともいずれかを介してＩＰパケットを受信した場合には、当該ＩＰパケットに基づいた所定の情報を当該ＩＰパケットの送信元に送信する、
ことを有し、上記エッジルータ及びコアルータによる経路制御処理により、上記サーバ実体により所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で論理的に区分けすることを特徴とする情報提供方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、例えば広域コンピュータネットワーク上で稼動する情報提供システム及び情報提供方法に係り、特に外部からの不正目的のアクセスによるシステム被害を局所化することで、情報提供サービス全体の攻撃耐性の向上と稼働率の向上を図る情報提供システム及び情報提供方法に関する。

【０００２】
【従来の技術】
従来、広域コンピュータネットワーク上では、複数のコンピュータにより構成される情報提供システムにより各種のサービスが提供されている。
【０００３】
このような情報提供システムでは、１つのサービスを同じ機能を有する複数のコンピュータ（以下、「サーバ実体」と称する）により提供している。更に、１つのサービスには、当該サービスを特定するネットワーク識別子（以下、「代表アドレス」と称する）が割り当てられている。そして、このような構成の下、当該情報提供システムでは、そのサービス提供中に、１つのサーバ実体が何らかの原因で停止した場合であっても、広域コンピュータネットワークを介して代表アドレスに向けられたユーザトラヒックを、稼動中の別のサーバ実体に自動的に振り分けることで、サービス自体を継続して提供することを可能としている。
【０００４】
例えば、従来の情報提供システムで用いられるＬ４スイッチでは、ＴＣＰやＵＤＰのポート番号等といったパケットのトランスポート層のヘッダ情報を読取って、当該ヘッダ情報に基づきパケットを転送している。即ち、このＬ４スイッチでは、ポート番号で識別したアプリケーション種類に応じて優先制御やフィルタリング、複数のサーバ実体を接続した環境での負荷分散等を実現している。
【０００５】
さらに、Ｌ７スイッチでは、ＵＲＬ等の第７層のヘッダ情報を基に、パケットの転送先を決めて転送処理をしている。即ち、このＬ７スイッチでは、アプリケーションそのものを認識してスイッチングする手法を採用することで、個々のアプリケーション毎に転送順位を設定することを可能としている。
【０００６】
一方、ＤＮＳ（ｄｏｍａｉｎ　ｎａｍｅ　ｓｙｓｔｅｍ）サーバが、クライアントであるＤＮＳリゾルバに対してＩＰアドレスを返答する際に、一つの名前に対して登録してある複数のＩＰアドレスを順番に返答するＤＮＳサーバの機能である「ＤＮＳラウンジロビン」が一般に知られている。このＤＮＳラウンジロビンによれば、複数のサイトにサーバ実体を分散配置する時に、エンドユーザ側に対して順繰りに回したＩＰアドレスを返答することで、広域でサーバの負荷を分散できる。
【０００７】
【発明が解決しようとする課題】
しかしながら、従来の技術では、外部からの不正目的のアクセスが代表アドレスに対して連続的に行われると、全てのサーバ実体が被害を受け、サービス提供が不可能になってしまう。それは、前述したように、従来技術に係る情報提供システムでは、上記不正目的のアクセスにより１つのサーバ実体が稼動不能になると、別のサーバ実体にトラヒックが自動的に振り分けられるためである。
【０００８】
このように、従来技術に係る情報提供システムでは、上記の如き不正目的のアクセスにより機能を停止したサーバ実体をバックアップするために、別の稼動中のサーバ実体に当該不正目的のアクセスに係るトラヒックが振り分けられることから、連鎖的にシステム内の全てのサーバ実体が被害を受けてしまう。
【０００９】
本発明は、上記問題に鑑みてなされたもので、その目的とするところは、広域コンピュータネットワーク上で複数のサーバ実体を分散配置して各サーバ実体にかかる負荷を分散しつつ所定のサービスを提供するような状況下において、当該広域コンピュータネットワークを介しての外部から不正目的のアクセスがなされることによるシステム被害、例えば、ＤＤｏＳ攻撃等の被害の影響を局所化することで、情報提供サービス全体の攻撃耐性の向上と稼働率の向上とを図る情報提供システム及び情報提供方法を提供することにある。

【００１０】
【課題を解決するための手段】
上記目的を達成するために、請求項１の発明では、広域ネットワーク上で稼動する情報提供システムにおいて、所定のネットワーク識別子が割り当てられており、上記広域ネットワーク上の対象に所定のサービスを提供するための複数の情報提供手段と、上記広域ネットワーク上の一のネットワークから他のネットワークへの経路制御処理について定義した第１のテーブルと、上記所定のネットワーク識別子を送信先とする情報の経路制御処理について定義した第２のテーブルと、を少なくとも有しており、上記第１又は第２のテーブルのいずれかを参照して経路制御処理を行うことで、上記各情報提供手段が上記所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で物理的に区分けするための経路制御手段と、を具備することを特徴とする情報提供システムが提供される。
【００１１】
請求項２の発明では、上記第２のテーブルは、上記所定のネットワーク識別子を送信先とする情報に対して、所定のラベルの付加、除去、変更をするラベル処理を行った後、所定の送信先に送信する旨、或いは、所定のラベルが付加された情報に対して、更なるラベル処理を行った後、所定の送信先に送信する旨、を少なくとも定義していることを更に特徴とする請求項１に記載の情報提供システムが提供される。
【００１２】
請求項３の発明では、上記所定のネットワーク識別子とはＩＰアドレスであり、上記経路制御処理手段は、上記所定のネットワーク識別子を送信先とするＩＰパケットを受信したときには、上記第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて定められる更なるラベル処理を行った後、所定の送信先に送信する、ことを更に特徴とする請求項２に記載の情報提供システムが提供される。
【００１３】
請求項４の発明では、広域ネットワーク上で稼動する情報提供システムにおいて、上記広域ネットワーク上の一のネットワークから他のネットワークへ送信すべきＩＰパケットを受信した場合には、第１のテーブルを参照して、当該ＩＰパケットを当該他のネットワークに送信し、一方、所定のサービスに係る所定のＩＰアドレスを送信先とするＩＰパケットを受信した場合には、第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて、当該ＩＰパケットに対して、所定のラベルの付加、除去、変更をするラベル処理を行った後に所定の送信先に送信する、エッジルータと、上記ラベル処理がなされたＩＰパケットを受信した場合には、第３のテーブルを参照して、当該ＩＰパケットに含まれる所定のラベルに基づいて定められる更なるラベル処理を行った後に所定の送信先に送信する、コアルータと、上記所定のサービスに係る所定のＩＰアドレスが割り当てられており、上記エッジルータ及びコアルータの少なくともいずれかを介してＩＰパケットを受信した場合には、当該ＩＰパケットに基づいた所定の情報を当該ＩＰパケットの送信元に送信する、複数のサーバ実体と、を有し、上記エッジルータ及びコアルータによる経路制御処理により、上記サーバ実体により所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で物理的に区分けすることを特徴とする情報提供システムが提供される。
【００１４】
請求項５の発明では、広域ネットワーク上で稼動する情報提供システムによる情報提供方法において、上記情報提供システムにより、上記広域ネットワーク上の一のネットワークから他のネットワークへ送信すべき情報を受信した場合には、第１のテーブルを参照して、当該情報を当該他のネットワークに送信するよう経路制御処理を行い、一方、所定のサービスに係る所定のネットワーク識別子を送信先とする情報を受信した場合には、第２のテーブルに基づく経路制御処理を行い、上記経路制御処理により、上記所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で論理的に区分けする、ことを特徴と

する情報提供方法が提供される。
【００１５】
請求項６の発明では、上記第２のテーブルは、上記所定のネットワーク識別子を送信先とする情報に対して、所定のラベルの付加、除去、変更をするラベル処理を行った後、所定の送信先に送信する旨、或いは、所定のラベルが付加された情報に対して、更なるラベル処理を行った後、所定の送信先に送信する旨、を少なくとも定義していることを更に特徴とする請求項５に記載の情報提供方法が提供される。
【００１６】
請求項７の発明では、上記所定のネットワーク識別子とはＩＰアドレスであり、上記情報提供システムにより、上記所定のネットワーク識別子を送信先とするＩＰパケットを受信したときには、上記第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて、当該ＩＰパケットに対して、所定のラベルの付加、除去、変更をするラベル処理を行った後、所定の送信先に送信することを更に特徴とする請求項６に記載の情報提供方法が提供される。
【００１７】
請求項８の発明では、エッジルータ、コアルータ、及びサーバ実体を有し、広域ネットワーク上で稼動する情報提供システムによる方法であって、上記エッジルータにより、上記広域ネットワーク上の一のネットワークから他のネットワークへ送信すべきＩＰパケットを受信した場合には、第１のテーブルを参照して、当該ＩＰパケットを当該他のネットワークに送信し、一方、所定のサービスに係る所定のＩＰアドレスを送信先とするＩＰパケットを受信した場合には、第２のテーブルを参照して、当該ＩＰパケットの、ＩＰアドレス、ＩＰアドレスとポート番号の組合せ、ＩＰアドレスとプロトコル番号の組合せ、の少なくともいずれかの情報に基づいて、当該ＩＰパケットに対して、所定のラベルの付加、除去、変更をするラベル処理を行った後に所定の送信先に送信し、上記コアルータにより、上記ラベル処理がなされたＩＰパケットを受信した場合には、第３のテーブルを参照して、当該ＩＰパケットに含まれる所定のラベルに基づいて定められる更なるラベル処理を行った後に所定の送信先に送信し、上記サーバ実体により、上記エッジルータ及びコアルータの少なくともいずれかを介してＩＰパケットを受信した場合には、当該ＩＰパケットに基づいた所定の情報を当該ＩＰパケットの送信元に送信する、ことを有し、上記エッジルータ及びコアルータによる経路制御処理により、上記サーバ実体により所定のサービスを提供する上記広域ネットワーク上の対象を所定単位で論理的に区分けすることを特徴とする情報提供方法が提供される。
【００１８】
【発明の実施の形態】
以下、図面を参照して、本発明の実施形態について説明する。
【００１９】
（第１実施形態）
先ず、図１乃至図６を参照しつつ、本発明の第１実施形態に係る情報提供システム及び情報提供方法について詳細に説明する。
【００２０】
図１には、第１実施形態に係る情報提供システムの構成を示し説明する。
【００２１】
この図１に示されるように、ネットワークN_X上には、複数のサーバ実体C_1乃至C_5が分散配置されている。そして、ネットワークN_Xの管理者が、複数のサーバ実体C_1乃至C_5によって１つのサービスＳを提供するために、当該サーバ実体C_1乃至C_5には、同じネットワーク識別子ｉｄｅｎｔｉｆｉｅｒが予め割り当てられている。さらに、上記サーバ実体C_1乃至C_5は、ルータR_1乃至R_{10}を介して、それぞれ通信自在に接続されており、ルータR_1乃至R_{10}を介して、外部のネットワークN_A乃至N_Cとも通信自在に接続されている。これらルータR_1乃至R_{10}は、パケットをユーザが期待する送信先

まで伝達する機能を有する。

【００２２】

ルータR_1、R_4、R_8、R_{10}はエッジルータであり、他はコアルータである。

【００２３】

以上のほか、ネットワークN_X内には、所定の利用ユーザU_1、U_2も存在しており、それぞれ二箇所のルータでトラヒックが収容されている。

【００２４】

このように、本発明の第１実施形態に係る情報提供システムは、所定のルーティング・ポリシによって運営されるネットワーク、即ち自律システム（ＡＳ；Ａｕｔｏｎｏｍｏｕｓ Ｓｙｓｔｅｍ）として構築されている。尚、ここでは、説明を簡略化するために、５個のサーバ実体C_1乃至C_5と１０個のルータR_1乃至R_{10}とを図示しているが、一例にすぎず、この数に限定されないことは勿論である。

【００２５】

尚、サーバ実体Ｃ１乃至Ｃ５は請求項に記載の情報提供手段の一例に相当し、ルータＲ１乃至Ｒ１０は請求項記載の経路制御処理手段の一例に相当する。

【００２６】

このような構成において、第１実施形態に係る情報提供システムでは、サービスＳを利用するユーザを、ネットワークN_Xに係る所定のルーティング・ポリシに従って、サーバ実体C_1乃至C_5の数だけグルーピングしている。

【００２７】

ここで、サービスＳを利用するユーザとは、例えば、ネットワークN_X内部のユーザU_1及びユーザU_2、外部ネットワークN_A乃至N_C内に存在するユーザ等を意味している。この例では、前述したように、ネットワークN_X内に５つのサーバ実体C_1乃至C_5が分散配置されているので、ネットワークN_X内のユーザU_1及びユーザU_2、ネットワークN_Aのユーザ、ネットワークN_Bのユーザ、ネットワークN_Cのユーザ、といった区分けで５つにグルーピングする。

【００２８】

即ち、各ユーザのトラフィックを、異なるサーバ実体C_1乃至C_5に振り分けるようなグルーピングを行う。尚、ユーザの数がサーバ実体の数よりも多い場合も当然に想定されるが、その場合には、例えばサーバ実体の数等により所定の区分けを行い、各ユーザのトラフィックを振り分けることになる。

【００２９】

次に、この情報処理システムでは、各サーバ実体C_1乃至C_5に向けた各ユーザグループのトラヒックが、ネットワークN_Xのどの資源を使用し、どの経路を通るかを決定する。この経路の決定は、ネットワークN_Xのネットワーク資源に追う時点ネットワーク管理者等が自由に決定することができる。

【００３０】

ここで、図２には、各サーバ実体C_1乃至C_5に対して、ユーザグループが使用する経路を決定した様子を概念的に示し説明する。この第１実施形態に係る情報提供システムでは、ネットワークN_X内の各ルータR_1乃至R_{10}により、サーバ実体C_1乃至C_5が送信先であるパケットの経路制御処理と、送信先がサーバ実体C_1乃至C_5でないパケットの経路制御処理とを分けて条件処理している。

【００３１】

そして、このような条件処理を実現するために、各ルータR_1乃至R_{10}は、詳細は後述するが、２つの経路制御処理テーブルを有している。

【００３２】

この情報処理システムでは、図３のフローチャートに示されるように、ルータR_1乃至R_{10}がパケットを受理すると（ステップＳ１）、当該パケットの送信先がサーバ実体C_1乃至C_5であるか否かを判断する（ステップＳ２）。送信先がサーバ実体C_1乃至C_5である場合は、通常の経路制御処理ではなく、ネットワーク管理者によって予め定められた

経路（例えば、図２に点領域で示されている経路）に沿ってパケットを転送し（ステップＳ４）、一方、送信先がサーバ実体C_1乃至C_5でない場合には、通常の経路制御処理を行う（ステップＳ３）。

【００３３】

例えば、図２において、ネットワークN_X内のユーザU_2からサーバ実体C_1乃至C_5（ネットワーク識別子ｉｄｅｎｔｉｆｉｅｒ）に向けたトラヒックは、予め定められた経路に沿って、即ちルータR_8，R_9を介してパケット転送され、サーバ実体C_3に到達し、他のサーバ実体C_1，C_2，C_4，C_5には転送されない。一方、ユーザU_2からのサーバ実体C_1乃至C_5（ネットワーク識別子Ｉｄｅｎｔｉｆｉｅｒ）以外、例えばネットワークN_A向けのトラヒックは、通常の経路制御処理によってネットワークN_Aまでパケットが順次転送されることになる。

【００３４】

以上の処理を実現するために、第１実施形態に係る情報提供システムでは、ネットワークN_X内にある全てのルータR_1乃至R_{10}が、図４（ａ），（ｂ）に示されるような２つの経路制御処理用テーブルを有するよう構成されている。

【００３５】

即ち、図４（ａ）に示したのは、本来的に全てのルータR_1乃至R_{10}が通常のパケット転送先を決定するための経路制御処理テーブルT_1である。この経路制御処理テーブルT_1では、送信先識別子とパケット転送先の識別子とが関係付けられて定義されている。一方、図４（ｂ）に示したのは、第１実施形態に係る情報提供システムで採用するサービスＳに係る転送先の定義する経路制御処理テーブルT_2である。この経路制御処理テーブルT_2では、サービスＳに係るネットワーク識別子ｉｄｅｎｔｉｆｉｅｒに対応するパケット転送先の識別子のみが定義されている。ネットワーク識別子ｉｄｅｎｔｉｆｉｅｒに対応するパケット転送先の識別子は、各ルータR_1乃至R_{10}が処理するグループのトラヒックとサービスＳを提供するサーバ実体C_1乃至C_5の位置に応じて設定されることになる。

【００３６】

尚、上記テーブルＴ１は、請求項記載の第１のテーブルの一例に相当し、上記テーブルＴ２は、請求項記載の第２、第３のテーブルの一例に相当する。

【００３７】

ここで、先に図３で示したルータR_1乃至R_{10}の処理フローは、経路制御テーブル参照処理であるから、図５に示すような手順で２つの経路制御処理テーブルを順番に参照することによって達成される。以下、これを詳述する。尚、この一連の処理は、情報提供方法の一例にも相当するものである。

【００３８】

ルータR_1乃至R_{10}のいずれかがパケットを受理すると（ステップＳ１１）、当該パケットのヘッダより送信先に係る情報を抽出する（ステップＳ１２）。

【００３９】

そして、ルータR_1乃至R_{10}のいずれかは、サービスＳに関する経路制御テーブル参照処理を行う（ステップＳ１３）。即ち、送信先がサービスＳに係るサーバ実体C_1乃至C_5（ネットワーク識別子ｉｄｅｎｔｉｆｉｅｒ）であるか否かを判断する（ステップＳ１３ａ）。そして、送信先がサーバ実体C_1乃至C_5であると判断した場合には、先に図４（ｂ）に示した経路制御処理テーブルT_2を参照して、対応するパケット転送先を特定し、当該転送先にパケットを転送する（ステップＳ１３ｂ）。一方、上記ステップＳ１３ａにて、送信先がサービスＳに係るサーバ実体C_1乃至C_5ではないと判断した場合には、先に図４（ａ）に示した通常の経路制御処理テーブルT_1を参照して、対応するパケット転送先に当該パケットを転送する（ステップＳ１４）。以上で、一連の処理を終了する。

【００４０】

以上説明した一連のルーティング制御により、ネットワークN_AからサービスＳへのトラヒックはサーバ実体C_1だけに送られるようになり、ネットワークN_BからサービスＳへ

のトラヒックはサーバ実体C_2だけに送られるようになる。さらに、サービスＳ以外のトラヒックは、従来と同様に通常の経路制御処理が行われる。つまり、サービスＳへのトラヒックに関する限り、図６に示すように、ユーザグループG_1乃至G_5毎に隔離することができる。

【００４１】

以上説明したように、第１実施形態に係る情報提供システムによれば、同一のサービスを提供するサーバ実体C_1乃至C_5に同一の代表アドレス（ｉｄｅｎｔｉｆｉｅｒ）を割り当て、通常の経路制御処理テーブルT_1と上記代表アドレスに対応した経路制御処理テーブルT_2とを使い分けるルータR_1乃至R_{10}により、ユーザトラフィックを各サーバ実体C_1乃至C_5に振り分けることで負荷を分散しつつ、広域コンピュータネットワークを介しての外部からの不正目的のアクセスによるシステム被害（例えば、ＤＤｏＳ攻撃等）を局所化し、情報提供サービス全体の攻撃耐性の向上と稼働率の向上とを図ることができる。

【００４２】

即ち、仮にネットワークN_A経由でコンピュータ犯罪者がサービスＳに対して攻撃を仕掛けてきた場合であっても、サーバ実体C_1は機能停止する可能性があるが、他のサーバ実体C_2乃至C_6は、影響を受けることなく、通常通りサービスを提供し続けることができる。また、その場合、ネットワークN_B，N_C、ユーザU_1、ユーザU_2に対しては、ネットワークN_A経由の攻撃の影響を完全に隠蔽することができる。また、仮に複数のコンピュータ犯罪者が協力してサービスＳに攻撃を仕掛けるとしても、ユーザグループ数のコンピュータ犯罪者が、ネットワーク管理者が独自に決めることができるユーザグループに必ず１名含まれていなければ全てのサーバ実体C_1乃至C_5の全て対して攻撃を仕掛けることができない。これは、事実上不可能であることから、前述したような構成、作用の第１実施形態に係る情報提供システムのコンピュータ犯罪者への攻撃耐性は極めて高くなるといえる。

【００４３】

（第２実施形態）

次に、図７乃至図１３を参照しつつ、本発明の第２実施形態に係る情報提供システム及び情報提供方法について詳細に説明する。

【００４４】

この第２実施形態では、広域ＩＰネットワークにおいて、何等かのサーバ（ＤＮＳやＷｅｂ等）を構築する例を想定している。ここでは、サーバ実体に割り当てられるネットワーク識別子、即ち「代表アドレス」はＩＰアドレスとなる。ＩＰアドレスは、ＩＰｖ４であってもＩＰｖ６であっても良い。

【００４５】

先ず、図７には第２実施形態に係る情報提供システムの構成を示し説明する。

【００４６】

この図７に示されるように、$ISP1_X$上には、複数のサーバ実体C_1乃至C_5が分散配置されている。そして、$ISP1_X$の管理者が、複数のサーバ実体C_1乃至C_5によって１つのサービスＳを提供するために、これらサーバ実体C_1乃至C_5には、同じネットワーク識別子、即ち、同じ代表アドレスが予め割り当てられている。これらサーバ実体C_1乃至C_5に割り当てられる代表アドレスは、$ISP1_X$が保持しているものであれば、いかなるものであってもよく、この第２実施形態では、例えば「１３６．１８７．１．１」という代表アドレスを使用する。

【００４７】

サーバ実体C_1乃至C_5は、ルータR_1乃至R_{10}を介して、それぞれ通信自在に接続されており、更にルータR_1乃至R_{10}を介して、外部の$ISP1_A$乃至1_Cとも通信自在に接続されている。これらルータR_1乃至R_{10}は、ＩＰパケットをユーザが期待する送信先まで伝達する機能を有するものである。サーバ実体C_1乃至C_5、ルータR_1乃至R_{10}の数は、これに限定されるものではない。

【００４８】
ＩＳＰ１$_{X}$の外部のＩＳＰ１$_{A}$乃至１$_{C}$は、ＡＳ番号を有している。これらＩＳＰ１$_{A}$乃至１$_{C}$は、ＡＳ間で利用するプロトコルであるＢＧＰ（Ｂｏｒｄｅｒ Ｇａｔｅｗａｙ Ｐｒｏｔｏｃｏｌ）に基づいてＩＰルーティングの経路情報を交換する。
【００４９】
以上のほか、上記ＩＳＰ１$_{X}$内には、所定の利用ユーザＵ$_{1}$、Ｕ$_{2}$も存在しており、それぞれ二箇所のルータでトラヒックが収容されている。また、この利用ユーザＵ$_{1}$又はＵ$_{2}$は、ＩＳＰ１$_{X}$に接続されている接続組織を意味する。尚、上記サーバ実体Ｃ$_{1}$乃至Ｃ$_{5}$は請求項に記載の情報提供手段の一例に相当し、上記ルータＲ$_{1}$乃至Ｒ$_{10}$は、請求項に記載の経路制御手段の一例に相当する。
【００５０】
このような構成において、ＩＳＰ１$_{X}$のネットワーク管理者は、各サーバ実体Ｃ$_{1}$乃至Ｃ$_{5}$に対するユーザグループを構成する。即ち、例えば、サーバ実体Ｃ$_{1}$にはＩＳＰ１$_{A}$の利用ユーザがアクセスし、サーバ実体Ｃ$_{2}$にはＩＳＰ１$_{X}$の利用ユーザＵ$_{1}$がアクセスし、サーバ実体Ｃ３にはＩＳＰ１$_{X}$の利用ユーザＵ$_{2}$がアクセスし、サーバ実体Ｃ$_{4}$にはＩＳＰ１$_{B}$の利用ユーザがアクセスし、サーバ実体Ｃ$_{5}$にはＩＳＰ１$_{C}$の利用ユーザがアクセスするように、ユーザグループを定義することになる。但し、ユーザグループは、この態様には限定されない。
【００５１】
続いて、ユーザグループが各サーバ実体Ｃ$_{1}$乃至Ｃ$_{5}$に到達するまでに通過すべき経路を決定し、そのような経路付け処理が行われるように各ルータＲ$_{1}$乃至Ｒ$_{10}$にて所定の設定を行う。この設定は、各ルータＲ$_{1}$乃至Ｒ$_{10}$に、該当ルータＲ$_{1}$乃至Ｒ$_{10}$からサーバ実体Ｃ$_{1}$乃至Ｃ$_{5}$まで、ＩＰ層によらないでパケット転送を行える機能を持たせることによって達成されることになる。
【００５２】
具体的には、各ルータＲ$_{1}$乃至Ｒ$_{10}$からサーバ実体Ｃ$_{1}$乃至Ｃ$_{5}$まで物理的な専用線を設定する第１の手法と、各ルータＲ$_{1}$乃至Ｒ$_{10}$において、ＩＰアドレスによらないラベルを設定し、当該ラベルに準じたパケット転送処理を行えるように設定する第２の手法等を採用し得る。そして、後者の第２の手法を実現する方式としては、ＭＰＬＳ（ｍｕｌｔｉｐｒｏｔｏｃｏｌ ｌａｂｅｌ ｓｗｉｔｃｈｉｎｇ）、ＧＭＰＬＳ（ｇｅｎｅｒａｌｉｚｅｄ ｍｕｌｔｉｐｒｏｔｏｃｏｌ ｌａｂｅｌ ｓｗｉｔｃｈｉｎｇ）、ＡＴＭ（Ａｓｙｎｃｈｒｏｎｏｕｓ Ｔｒａｎｓｆｅｒ Ｍｏｄｅ）のＶＣ（Ｖｉｒｔｕａｌ Ｃｈａｎｎｅｌ）設定、等が挙げられる。
【００５３】
ここで、ＭＰＬＳとは、ＩＰネットワークで使うカット・スルー方式のパケット転送技術であり、ラベル・スイッチング技術とも称される。このＭＰＬＳではＩＰパケット内にラベルという識別子を挿入し、当該ラベルと経路の対応を管理するＩＰネットワーク上のＭＰＬＳ対応ノードがラベルによってパケットを高速転送することで、トラヒックの負荷分散等を実現する。ラベルは、シム・ヘッダと称されるＭＰＬＳ専用のヘッダの形でＩＰパケットの第２層ヘッダと第３層ヘッダの間に挿入される。尚、ＭＰＬＳにおいてパケットが配送される経路はＬＳＰ（Ｌａｂｅｌ Ｓｗｉｔｃｈ Ｐａｔｈ）と称される。ＧＭＰＬＳはＭＰＬＳのラベル配送の技術を光の波長やＴＤＭにおけるタイムスロット等に拡張するものである。どちらの場合においても、ＣＲ－ＬＤＰ等の明示的なＬＳＰ設定が可能なラベル配布プロトコルを使用してパケット配送に必要な情報の交換を行う。
【００５４】
そして、ＡＴＭのＶＣ設定とは、ＭＰＬＳにおけるＬＳＰをＡＴＭにおけるＶＣの機能で実現するものである。
【００５５】
以下、ＭＰＬＳを採用した第２実施形態の実装例について詳細に説明する。
【００５６】

この例では、ルータR_1乃至R_4は、それぞれＭＰＬＳ機能を有しており、ＬＳＲとして動作することを前提としている。ここで、ＬＳＲとは、ＭＰＬＳを解釈できるルータ（ＭＰＬＳエッジルータ、ＭＰＬＳコアルータ）をいう。

【００５７】

ルータR_1は、送信先がＩＰアドレス１３６．１８７．１．１であるＩＰパケットについてはＭＰＬＳのラベルを付加し、ルータR_2に送信する。そして、それ以外のＩＰアドレスを送信先とするＩＰパケットについては、通常のＡＳ内部で使用されるルーティングプロトコルであるＩＧＰ（Ｉｎｔｅｒｉｏｒ Ｇａｔｅｗａｙ Ｐｒｏｔｏｃｏｌ）によるルーティングに委ねるように設定を行っている。

【００５８】

ここで、ルータR_1の有する経路制御処理テーブルは、図９（ａ），（ｂ）に示される。これは、第１実施形態で説明した図４に対応するものである。

【００５９】

図９（ａ）に示されるように、通常の経路制御処理テーブルは、ＩＧＰ及びＢＧＰ（Ｂｏｒｄｅｒ Ｇａｔｅｗａｙ Ｐｒｏｔｏｃｏｌ）によって得られたものであり、送信先とパケット転送先のＩＰアドレスが対応付けられている。

【００６０】

一方、図９（ｂ）に示されるように、ＭＰＬＳのＦＩＢ（Ｆｏｒｗａｒｄｉｎｇ Ｉｎｆｏｒｍａｔｉｏｎ Ｂａｓｅ）のうちＦＴＮ（ＦＥＣ ｔｏ ＮＨＬＦＥ）は、何らかのラベル配布手順、例えばＣＲ－ＬＤＰ（Ｃｏｎｓｔｒａｉｎｔ－Ｂａｓｅｄ ＬＤＰ）やＲＳＶＰ－ＴＥ（Ｒｅｓｏｕｒｃｅ Ｒｅｓｅｒｖａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｔｒａｆｆｉｃ Ｅｎｇｉｎｅｅｒｉｎｇ Ｅｘｔｅｎｓｉｏｎ）等によって得られたものである。

【００６１】

ＣＲ－ＬＤＰは、ＬＤＰを拡張したものであり、プレフィックスベースと異なり、あるルータ間で個別にラベルパスを作る方式である。

【００６２】

そして、ＲＳＶＰ－ＴＥは、ラベル付与リクエストを隣接ルータに対して送信し、リクエストを受け取ったルータが、その内容に応じて該当のプレフィックス等にラベルを付与するものである。即ち、要求のあったプレフィックスに対してのみ個々にラベルを付与する方式である。

【００６３】

ＦＴＮは、ＦＥＣ（Ｆｏｒｗａｒｄｉｎｇ Ｅｑｕｉｖａｌｅｎｃｅ Ｃｌａｓｓ）とＮＨＬＦＥ（Ｎｅｘｔ Ｈｏｐ Ｌａｂｅｌ Ｆｏｒｗａｒｄｉｎｇ Ｅｎｔｒｙ）との関係を示すテーブルである。

【００６４】

ＦＥＣは、送信先のグループエントリの一つを示している。

【００６５】

そして、ＮＨＬＦＥでは、ラベルが付加されていないパケットに所定のラベルを付加したり（コマンド：ラベルＰＵＳＨ）、既にラベルが付加されているパケットのラベルを除去したり（コマンド：ラベルＰＯＰ）、ラベル付きパケットのラベルを交換したり（コマンド：ラベルＳＷＡＰ）、とった内容を示している。

【００６６】

例えば、図９（ｂ）のＦＴＮでは、ＦＥＣには「１３６．１８７．１．１」とあるが、これは送信先アドレスが「１３６．１８７．１．１」であることを意味している。

【００６７】

また、ＮＨＬＦＥには「ラベルＰＵＳＨ、ラベル＃１３６」とあるが、これは識別番号として１３６が割り当てられたラベルをパケットに付加することを意味している。これを「ラベル＃１３６」と記述することにする。更に、ＮＨＬＦＥには「Ｆｏｒｗａｒｄ＝１５０．１００．９．１」とあるが、これはラベル＃１３６を付加したパケットの転送先のＩ

Ｐアドレスが１５０．１００．９．１であることを意味している。
【００６８】
尚、ＭＰＬＳのＦＩＢには、一般にラベルとＮＨＬＦＥとの関係を示すＩＬＭ（Ｉｎｃｏｍｉｎｇ　Ｌａｂｅｌ　Ｍａｐｐｉｎｇ）も含まれるが、この例では説明の便宜上、当該ルータ$Ｒ_1$においてはＩＬＭが設定されていないものとする。
【００６９】
尚、図９（ａ）のテーブルは請求項記載の第１のテーブルの一例に相当し、図９（ｂ）のテーブルは請求項記載の第２のテーブルの一例に相当する。
【００７０】
同様に、ルータ$Ｒ_2$の有する経路制御処理テーブルは、図１０（ａ），（ｂ）に示される。これは、第１実施形態で説明した図４に対応する。
【００７１】
図１０（ａ）に示されるように、通常の経路制御処理テーブルは、ＩＧＰ及びＢＧＰ（Ｂｏｒｄｅｒ　Ｇａｔｅｗａｙ　Ｐｒｏｔｏｃｏｌ）によって得られたものであり、送信先とパケット転送先のＩＰアドレスが対応付けられている。
【００７２】
一方、図１０（ｂ）に示されるように、ＭＰＬＳのＩＬＭは、送信されてきたパケットに貼られているラベルとＮＨＬＦＥとの関係を示している。
【００７３】
ここでも、ＮＨＬＦＥでは、ラベルが付加されていないパケットに所定のラベルを付加したり（コマンド：ラベルＰＵＳＨ）、既にラベルが付加されているパケットのラベルを除去したり（コマンド：ラベルＰＯＰ）、ラベル付きパケットのラベルを交換したり（コマンド：ラベルＳＷＡＰ）、とった内容を示している。
【００７４】
例えば、図１０（ｂ）のＩＬＭでは、Ｉｎｃｏｍｉｎｇ　Ｌａｂｅｌには「＃１３６」とあるが、これは受信したラベル付きパケットに付加されていたラベルの識別番号が１３６であることを意味している。
【００７５】
また、ＩＬＭのＮＨＬＦＥには「ラベルＰＯＰ、Ｆｏｒｗａｒｄ＝１３６．１８７．１．１」とあるが、これはラベル＃１３６をパケットより除去した後に、ＩＰアドレス１３６．１８７．１．１に転送することを意味している。この例では、ルータ$Ｒ_2$においては説明の便宜上、ＦＴＮが設定されていないものとする。尚、図１０（ｂ）のテーブルは、請求項に記載の第３のテーブルの一例に相当する。
【００７６】
次に図１１（ａ），（ｂ）を参照して、ラベル情報の付加について説明する。
【００７７】
尚、この例では、ネットワークは、広域イーサネット専用線を使用しているものと仮定している。さて、図８のＩＳＰ１_AからＩＰアドレス１３６．１８７．１．１に向けたフレームは、物理ヘッダ、ＩＰヘッダ、ＩＰデータを有している。
【００７８】
そして、ＩＰパケットは、ルータ$Ｒ_1$において図１１に示されるようにラベル付けされる。すなわち、図１１（ａ），（ｂ）に示されるように、ラベル付け処理は、ネットワークメディアのレイヤ２ヘッダ中の上位プロトコルを示すＴｙｐｅフィールド値をＩＰを示す０ｘ０８００からＭＰＬＳユニキャストパケットラベルを示す０ｘ８８４７に書き換え、更にＭＰＬＳのラベル情報を包含するシム・ヘッダを挿入することによって行われる。なお、他のネットワーク媒体を使用する場合であっても、レイヤ２ヘッダのフォーマット及びフィールド値には違いはあるものの基本的に上位プロトコルを示す値がＩＰを示すものからＭＰＬＳユニキャストパケットラベルを示すものに書き換わる点に相違はない。
【００７９】
一方で、図８のＩＳＰ１_Aから他の送信先、例えばＩＳＰ１_Xを経由してＩＳＰ１_B（Ｉ

Ｐアドレス１６０．１６０．１６０．１６０）に向かうパケットについては、ラベル付け処理は行われない。従って、この場合、レイヤ２ヘッダのＴｙｐｅフィールド値は書き換えられず、フィールド値は０ｘ０８００に維持される。

【００８０】

以下、図９（ａ），（ｂ）、及び図１２のフローチャートを参照して、第２実施形態に係る情報提供システムにおけるルータR_1（ＭＰＬＳエッジルータ）の経路制御テーブル参照処理について更に詳細に説明する。

【００８１】

尚、この一例の処理は、情報提供方法の一例にも相当するものである。

【００８２】

ルータR_1は、ＩＰパケットをデータとして有する物理フレームを受理すると（ステップＳ２１）、当該ＩＰパケットの物理ヘッダのＴｙｐｅフィールド値がＩＰを示す０ｘ０８００であるか否かを判断する（ステップＳ２２）。このステップＳ２２において、ルータR_1は、Ｔｙｐｅフィールド値が０ｘ０８００ではないならば、エラーとしてＩＰパケットを破棄し（ステップＳ２３）、本処理を終了する。

【００８３】

一方、ルータR_1は、Ｔｙｐｅフィールド値が０ｘ０８００であるならば、ＩＰヘッダの送信先アドレスを抽出する（ステップＳ２４）。そして、サービスＳに関する経路制御テーブル参照処理に移行する（ステップＳ２５）。

【００８４】

即ち、ルータR_1は、送信先が代表アドレス「１３６．１８７．１．１」であるか否かを判断し（ステップＳ２５ａ）、１３６．１８７．１．１である場合には、先に図９（ｂ）に示したＦＩＢを参照し、ＦＴＮの１３６．１８７．１．１に対応するＮＨＬＦＥに従い、ＩＰパケットのＴｙｐｅフィールド値をＭＰＬＳユニキャストパケットラベルを示す０ｘ８８４７に書き換えた後、シム・ヘッダとしてラベル情報を追加し、当該ラベル付きのＩＰパケットを転送し（ステップＳ２５ｂ）、本処理を終了する。

【００８５】

一方、上記ステップＳ２５ａにて、送信先が１３６．１８７．１．１でない場合には、先に図９（ａ）に示した通常の経路制御テーブルを参照し、対応するパケット転送先にパケット転送処理を行い（ステップＳ２６）、本処理を終了する。

【００８６】

次に、図１３のフローチャートを参照して、第２実施形態に係る情報提供システムにおけるルータR_2（ＭＰＬＳコアルータ）の経路制御テーブル参照処理について更に詳細に説明する。尚、この一連の処理は、情報提供方法の一例にも相当するものである。

【００８７】

ルータR_2は、ＩＰパケットをデータとして有する物理フレームを受理すると（ステップＳ３１）、当該ＩＰパケットの物理ヘッダのＴｙｐｅフィールド値がＩＰを示す０ｘ０８００であるか否かを判断する（ステップＳ３２）。

【００８８】

このステップＳ３２において、ルータR_2は、Ｔｙｐｅフィールド値がＩＰを示す０ｘ０８００ではないならば、Ｔｙｐｅフィールド値がＭＰＬＳユニキャストパケットラベルを示す０ｘ８８４７であるか否かを判断する（ステップＳ３５）。

【００８９】

そして、ステップ３５にて、Ｔｙｐｅフィールド値が０ｘ８８４７でないならば、エラーとしてＩＰパケットを破棄し（ステップＳ３６）、本処理を終了する。

【００９０】

一方、ルータR_2は、Ｔｙｐｅフィールド値が０ｘ８８４７であるならば、サービスＳに関する経路制御テーブル参照処理に移行する（ステップＳ３７）。

【００９１】

即ち、ルータR_2は、送信先がラベル＃１３６であるか否かを判断する（ステップＳ３７

ａ）。ステップＳ３７ａにおいて、ラベル＃１３７である場合、先に図１０（ｂ）に示したＦＩＢを参照し、ＬＩＭのラベル＃１３７に対応するＮＨＬＦＥに従いＩＰパケットのラベル＃１３７を除去した後、ＩＰパケットをＩＰアドレス１３６．１８７．１．１に転送し（ステップＳ２５ｂ）、本処理を終了する。上記ステップＳ３７ａにて、送信先がラベル＃１３７でない場合、エラーとしてＩＰパケットを破棄し（ステップＳ３７ｂ）、本処理を終了することになる。

【００９２】

一方、上記ステップＳ３２にて、送信先がＴｙｐｅフィールド値がＩＰを示す０ｘ０８００であると判断した場合には、ルータR_2は、ＩＰパケットよりＩＰヘッダの送信先アドレスを抽出し（ステップＳ３３）、先に図１０（ａ）に示した通常の経路制御テーブルを参照して、上記送信先アドレスに対応するパケット転送先にパケット転送処理を行い（ステップＳ３４）、本処理を終了する。

【００９３】

以上説明したように、第２実施形態によれば、同一のサービスを提供する複数のサーバ実体C_1乃至C_5が分散配置された情報提供システムにおいて、例えばＭＰＬＳ機能を有するＭＰＬＳエッジルータR_1、R_4、R_8、R_{10}及びＭＰＬＳコアルータR_2、R_3、R_5、R_6、R_7、R_9を多数配置し、当該ルータに通常の経路制御処理テーブルとＭＰＬＳのＦＩＢとを持たせ、各ルータR_1乃至R_{10}が当該テーブルによりＩＰパケットをサーバ実体C_1乃至C_5に振り分けることで、負荷を分散しつつ、広域コンピュータネットワークを介しての外部からの不正目的のアクセスによるシステム被害（例えば、ＤＤｏＳ攻撃等）を局所化し、情報提供サービス全体の攻撃耐性の向上と稼働率の向上とを図ることができる。

【００９４】

即ち、第２実施形態では、仮に$ISP1_A$からＤＤｏＳ攻撃があった場合、全てのトラヒックはサーバ実体C_1へと集中する。その結果、サーバ実体C_1はダウンするが、他のサーバ実体C_2乃至C_5は、継続して動作することができる。また、サーバ実体C_1のダウンは、$ISP1_B$のユーザ、$ISP1_C$のユーザ、$ISP1_X$内のユーザU_1、ユーザU_2からは分らない。さらに、仮に$ISP1_B$からサーバ実体C_1をダウンさせようとしても、$ISP1_B$からサーバ実体C_1にＩＰパケットを到達させることはできない。また、仮にＩＰソースルートを設定して１５０．１００．７．１経由で１３６．１８７．１．１にパケットを到達させようとしても、ルータR_2は１３６．１８７．１．１のＩＰ経由エントリを有しないため１３６．１８７．１．１へはパケットを到達させることはできないこととなる。

【００９５】

（第３実施形態）

次に、図１４乃至図２１を参照しつつ、本発明の第３実施形態に係る情報提供システム及び情報提供方法について詳細に説明する。

【００９６】

この第３実施形態では、第２実施形態と同様に、広域ネットワークである$ISP1_X$上で自律システムを構築する場合を考える。また、第２実施形態においては、一つのサービスに一つの代表アドレスが設定される例を示したが、第３実施形態では、一つの代表アドレスによって複数のサービスを提供し、各サービスについてＤＤｏＳ攻撃によるサーバダウンの範囲を局所化する。即ち、広域コンピュータネットワーク上で複数のサーバ実体を分散配置して各サーバ実体にかかる負荷を分散しつつ所定のサービスを提供するような状況下において、当該広域コンピュータネットワークを介しての外部から不正目的のアクセスがなされることによるシステム被害、例えば、ＤＤｏＳ攻撃等の被害の影響を局所化することで、情報提供サービス全体の攻撃耐性の向上と稼働率の向上とを図ることに特徴を有する点は、前述した第１及び第２の実施形態と同様である。

【００９７】

尚、本発明の第３実施形態に係る情報提供システムの構成は、先に第２実施形態として説

明した図７と略同様であるので、ここでは図７を適宜参照しつつ、更に同一構成要素には同一符号を用いて説明する。各構成と、請求項との関係についても、第２実施形態で前述したのと略同様である。

【００９８】

第３実施形態では、第２実施形態と同様に、ＩＳＰ１$_X$のネットワーク管理者は、各サーバ実体に対するユーザグループを構成する。

【００９９】

そして、第３実施形態では、例えば「ホームページ閲覧（ＨＴＴＰ）はサーバ実体Ｃ$_1$を使用し、ファイルダウンロード（ＦＴＰ）はサーバ実体Ｃ$_4$を使用する」といった選択をすることもできる。つまり、同じ代表アドレスを使用しながらサービスによって使用するサーバ実体を変更することができる。

【０１００】

ここで、図１４には、図８と略同様である第３実施形態に係る情報提供システムの一部拡大図を示して説明する。

【０１０１】

図１４に示されるように、ＩＳＰ１$_A$のユーザに対して、ホームページ閲覧（ＨＴＴＰ）はサーバ実体Ｃ$_1$、ファイルダウンロード（ＦＴＰ）はサーバ実体Ｃ$_4$を選択するようにユーザトラヒックがグループ分けされる。次いで、ユーザグループが各サーバ実体Ｃ$_1$乃至Ｃ$_5$に至までに通過する経路を決定し、そのような経路付け処理が行われるようにネットワークの設定を行う。それ以外のトラヒックについては、通常のＩＧＰルーティングに委ねるべく設定を行う。

【０１０２】

以下、ＭＰＬＳを採用した第３実施形態の実装例について詳細に説明する。

【０１０３】

この例では、ルータＲ$_1$乃至Ｒ$_4$は、それぞれＭＰＬＳ機能を有しており、ＬＳＲとして動作することを前提としている。ここで、ＬＳＲとは、ＭＰＬＳを解釈できるルータ（ＭＰＬＳエッジルータ、ＭＰＬＳコアルータ）をいう。

【０１０４】

ここで、ルータＲ$_1$の有する経路制御処理テーブルは、図１５（ａ），（ｂ）に示される。これは、第１実施形態で説明した図４に対応するものである。

【０１０５】

図１５（ａ）に示されるように、通常の経路制御処理テーブルは、ＩＧＰ及びＢＧＰによって得られたものであり、送信先とパケット転送先のＩＰアドレスが対応付けられている。そして、図１５（ｂ）に示されるように、ＭＰＬＳのＦＩＢのうちＦＴＮは、何らかのラベル配布手順、例えばＣＲ－ＬＤＰやＲＳＶＰ－ＴＥを拡張し、ＩＰアドレスに加えてプロトコル番号、ポート番号を組み合せて得られる。先に説明した第２実施形態との違いは、このようなＭＰＬＳのＦＩＢの持たせ方にある。即ち、先に説明した第２実施形態ではＩＰアドレスに対して１つのラベルが設定されているが、第３実施形態では、１つのプロトコルポートに対して１つのラベルが設定される。詳細には、ＨＴＴＰではＴＣＰ／８０を使用するため、１つのプロトコルポートに対して１つのラベルを設定する。これに対して、ＦＴＰではＴＣＰ／２０、ＴＣＰ／２１両方を使用するために、２つのプロトコルポートに対して１つのラベルを設定する。

【０１０６】

例えば、図１５（ｂ）のＦＴＮは、送信先アドレスが１３６．１８７．１．１でありプロトコルポートがＴＣＰ／８０である場合には、ラベル＃１３６を付加したパケットを、ＩＰアドレス１５０．１００．９．１に転送することを意味している。さらに、ＦＴＮの送信先アドレスが１３６．１８７．１．１でありプロトコルポートがＴＣＰ／２０，ＴＣＰ／２１である場合には、ラベル＃１３７を付加したパケットを、ＩＰアドレス１５０．１００．９．１に転送することを意味している。

【０１０７】

ここで、ＭＰＬＳのＦＩＢには、一般にラベルとＮＨＬＦＥとの関係を示すＩＬＭも含まれるが、この例では、説明の便宜上、当該ルータ$Ｒ_1$においてはＩＬＭが設定されていないものとする。尚、図１５（ａ）のテーブルは請求項記載の第１のテーブルの一例に相当し、図１５（ｂ）のテーブルは請求項記載の第２のテーブルの一例に相当するものである。

【０１０８】

同様に、ルータ$Ｒ_2$の有する経路制御処理テーブルは、図１６（ａ），（ｂ）に示される。これは、第１実施形態で説明した図４に対応するものである。

【０１０９】

図１６（ａ）に示されるように、通常の経路制御処理テーブルは、ＩＧＰ及びＢＧＰによって得られたものであり、送信先とパケット転送先のＩＰアドレスが対応付けられている。一方、図１６（ｂ）に示されるように、ＭＰＬＳのＩＬＭは、送信されてきたパケットに貼られているラベルとＮＨＬＦＥとの関係を示している。例えば、図１０（ｂ）のＩＬＭでは、ＩＰパケットに付加されたラベルが＃１３６である場合には、当該ラベル＃１３６を除去した後、ＩＰアドレス１３６．１８７．１．１に転送することを意味している。更に、ＩＰパケットに付加されたラベルが＃１３７である場合には、当該ラベルを新たなラベル＃２３７に変更した後に、ＩＰアドレス１５０．１００．７．２に転送することを意味している。

【０１１０】

ここでは、説明の便宜上、ルータ$Ｒ_2$においては、ＦＴＮが設定されていないものとする。尚、図１６（ｂ）のテーブルは請求項記載の第３のテーブルの一例に相当するものである。

【０１１１】

同様に、ルータ$Ｒ_3$の有する経路制御処理テーブルは、図１７（ａ），（ｂ）に示される。これは、第１実施形態で説明した図４に対応するものである。

【０１１２】

図１７（ａ）に示されるように、通常の経路制御処理テーブルは、ＩＧＰ及びＢＧＰによって得られたものであり、送信先とパケット転送先のＩＰアドレスが対応付けられている。一方、図１７（ｂ）に示されるように、ＭＰＬＳのＩＬＭは、送信されてきたパケットに貼られているラベルとＮＨＬＦＥとの関係を示している。例えば、図１７（ｂ）のＩＬＭでは、ＩＰパケットに付加されたラベルが＃２３７である場合には、当該ラベル＃２３７を除去した後、ＩＰアドレス１３６．１８７．１．１に転送することを意味している。ここでは、説明の便宜上、ルータ$Ｒ_3$においてはＦＴＮが設定されていないものとする。尚、図１７（ｂ）のテーブルは請求項記載の第３のテーブルの一例に相当するものである。

【０１１３】

ここで、前述したようにＩＰアドレスに加えてプロトコル番号、ポート番号を基にラベルを配布するためには、既存のラベル配布手順を拡張する必要がある。

【０１１４】

以下、図１８を参照して、ＣＲ－ＬＤＰを利用してラベルを配布する例を説明する。これは、本発明のラベル配布方法に相当するものである。

【０１１５】

ＣＲ－ＬＤＰでは、Ｄｏｗｎｓｔｒｅａｍ ｏｎ Ｄｅｍａｎｄ型ラベル配布方式と、Ｏｒｄｅｒｅｄ ＬＳＰ制御方式を組み合せる。尚、このＤｏｗｎｓｔｒｅａｍ ｏｎ Ｄｅｍａｎｄ型ラベル配布方式とはラベル付与要求のあったときのみラベルを割り付けるものである。

【０１１６】

この図１８に示されるように、サーバ実体$Ｃ_1$（１３６．１８７．１．１，ＴＣＰ／８０）に対応するラベル配布は、ルータ$Ｒ_1$が明示ルート（ＥＲ－Ｒｏｕｔｅ）ＴＬＶによって明示的に通過するルータを指定（ルータ$Ｒ_1$－ルータ$Ｒ_2$の場合は直接接続なのでルー

タR_2のみが指定される）したラベル要求メッセージをルータR_2に送信し、ルータR_2がラベル割当てメッセージをルータR_1に返すことで行われる。

【０１１７】

これに対して、サーバ実体C_4（１３６．１８７．１．１，ＴＣＰ２０，ＴＣＰ２１）に対応するラベル配布は、ルータR_1が明示ルート（ＥＲ－Ｒｏｕｔｅ）ＴＬＶによって通過すべきルータがルータR_2からルータR_3である旨が明示的に指定されたラベル要求メッセージをルータR_3に送信し、当該ルータR_3によって送信されたラベル割当てメッセージがルータR_1に到着することで行われることになる。

【０１１８】

ここで、このサーバ実体C_4のＴＣＰ／２０にラベルが割り当てられるまでの詳細な手順は、図１９に示される通りである。以下、これを詳述する。

【０１１９】

即ち、ルータR_1よりルータR_2に対してラベル要求メッセージにより１３６．１８７．１．１，ＴＣＰ／２０のラベルがリクエストされると（＃１）、ルータR_2は、ルータR_3に対してラベル要求メッセージを転送し、１３６．１８７．１．１，ＴＣＰ／２０のラベルをリクエストする（＃２）。ルータR_3は、ラベル＃２３７を割り当て、ＩＬＭを図１９に符号T_{10}で示すような内容に設定する（＃３）。即ち、ＩＬＭを、転送されたＩＰパケットにラベル＃２３７が貼られている場合には、当該ラベル＃２３７を剥がし、１３６．１８７．１．１に転送するような内容に設定する。

【０１２０】

続いて、ルータR_3は、ラベル＃２３７の情報をラベル割当てメッセージによりルータR_2に送信する（＃４）。ルータR_2は、ラベル割当てメッセージを受信すると、ＦＥＣ１３６．１８７．１．１，ＴＣＰ／２０の出力ラベル＃２３７に対して入力ラベル＃１３７を割り当て、ＩＬＭを図１９に符号T_{11}で示すような内容に設定する（＃５）。即ち、ルータR_2は、ＦＩＢのＩＬＭを、転送されたＩＰパケットにラベル＃１３７が貼られている場合には、当該ラベル＃１３７をラベル＃２３７に変更し、１５０．１００．７．２に転送するような内容に設定することとしている。

【０１２１】

次いで、ルータR_2は、ラベル＃１３７の情報をラベル割当てメッセージによりルータR_1に返信する（＃６）。ルータR_1は、ラベル割当てメッセージを受信すると、ＦＴＮを図１９において符号T_{12}で示すような内容に設定する。即ち、送信先のＩＰアドレスが１３６．１８７．１．１，ＴＣＰ／２０である場合には、ラベル＃１３７を貼り、１５０．１００．８．１に転送するような内容に設定する。以上により、サーバ実体C_4のＴＣＰ／２０にラベルが割り当てられる。

【０１２２】

即ち、本発明の実施の形態に係るラベル配布方法では、エッジルータが少なくとも所定のＩＰアドレス、ポート番号により送信先が特定されるＩＰパケットに関するラベルをコアルータに対してラベル要求メッセージにより要求すると、コアルータが所定のラベルを割り当てて自己のＩＬＭの内容を設定し、当該ラベルの情報をラベル割当てメッセージによりエッジルータに送信する。エッジルータは、このラベル割当てメッセージを受信すると、上記ＩＰパケットの少なくともＩＰアドレス及びポート番号と、ラベルとを対応付けるようにＦＴＮの内容を設定する。尚、エッジルータが明示ルート（ＥＲ－Ｒｏｕｔｅ）ＴＬＶによって通過すべきルータが存在する場合、ラベル要求メッセージによりその旨が示される。

【０１２３】

ところで、従来のＣＲ－ＬＤＰでは、１つのラベルに対応するＦＥＣはＩＰプレフィックスだけとなっている。しかし、第３実施形態では、ＩＰプレフィックスに加えて上位層（ＴＣＰ，ＵＤＰのポート番号）を必要とするため、ＬＤＰ，ＣＲ－ＬＤＰ双方で共通して使用しているＦＥＣ　ＴＬＶ部分を拡張する。

【０１２４】

ここで、図２０（ａ）は一般的なＦＥＣ　ＴＬＶのフォーマットを示している。

【０１２５】

即ち、図２０（ａ）に示されるように、一般的なＦＥＣ　ＴＬＶのフォーマットのＦＥＣ記述フィールドには、以下の４種類が規定されている。

【０１２６】

０ｘ０１　；　ワイルドカード
０ｘ０２　；　ＩＰプレフィックス
０ｘ０３　；　ホストアドレス
０ｘ０４　；　ＣＲ－ＬＳＰ

そして、第３実施形態では、これらに加えて、新たにタイプ０ｘ０５（タイプ：ソケット）を定義する。このタイプ０ｘ０５のＴＬＶフォーマットは、図２０（ｂ）に示される通りである。以上のような拡張により、ＣＲ－ＬＤＰを利用したアプリケーション別のラベル配布を可能としている。

【０１２７】

以下、図１５（ａ），（ｂ）、及び図２１のフローチャートを参照して、第３実施形態に係る情報提供システムにおけるルータR_1（ＭＰＬＳエッジルータ）の経路制御テーブル参照処理について更に詳細に説明する。

【０１２８】

先ず、ルータR_1は、ＩＰパケットをデータとして有する物理フレームを受理すると（ステップＳ４１）、当該ＩＰパケットの物理ヘッダのＴｙｐｅフィールド値がＩＰを示す０ｘ０８００であるか否かを判断する（ステップＳ４２）。このステップＳ４２において、ルータR_1は、Ｔｙｐｅフィールド値が０ｘ０８００ではないならば、エラーとしてＩＰパケットを破棄し（ステップＳ４３）、本処理を終了する。

【０１２９】

一方、ルータR_1は、Ｔｙｐｅフィールド値が０ｘ０８００であるならば、ＩＰヘッダの送信先アドレスを抽出する（ステップＳ４４）。そして、サービスＳに関する経路制御テーブル参照処理に移行する（ステップＳ４５）。

【０１３０】

即ち、ルータR_1は、送信先が代表アドレス「１３６．１８７．１．１」であるか否かを判断し（ステップＳ４５ａ）、１３６．１８７．１．１である場合には、ポート番号がＴＣＰ／８０、ＴＣＰ／２０、ＴＣＰ／２１のいずれかであるかを判断する（ステップＳ４５ｂ）。そして、いずれでもない場合には、エラーとしてＩＰパケットを破棄し（ステップＳ４５ｃ）、本処理を終了する。一方、ポート番号がＴＣＰ／８０、ＴＣＰ／２０、ＴＣＰ／２１のいずれかである場合には、先に図１５（ｂ）に示したＦＩＢを参照し、ＦＴＮの１３６．１８７．１．１に対応するＮＨＬＦＥに従い、ＩＰパケットのＴｙｐｅフィールド値をＭＰＬＳユニキャストパケットラベルを示す０ｘ８８４７に書き換えた後、シム・ヘッダとしてラベル情報を追加し、当該ラベル付きのＩＰパケットを転送し（ステップＳ４５ｄ）、本処理を終了する。

【０１３１】

一方、上記ステップＳ４５ａにて、送信先が１３６．１８７．１．１でない場合には、先に図１５（ａ）に示した通常の経路制御テーブルを参照し、対応するパケット転送先にパケット転送処理を行い（ステップＳ４６）、本処理を終了する。

【０１３２】

以上説明したように、第３実施形態では、１つの代表アドレスが与えられた複数のサーバ実体Ｃ１乃至Ｃ５によって複数のサービス（例えば、ホームページ閲覧（ＨＴＴＰ）とファイルダウンロード（ＦＴＰ）の如く）を提供し、各サービスについてＤＤｏＳ攻撃によるサーバダウンの範囲を局所化することができる。

【０１３３】

即ち、第３実施形態では、仮にＩＳＰ1_AからＳｍｕｒｆ攻撃として知られる大量のＩＣＭＰを使用したＤＤｏＳ攻撃、或いは巨大なデータサイズを持つＵＤＰを使用した攻撃が

あったとしても、各サーバ実体C_1乃至C_5には指定のＴＣＰポートを使用していない限りラベルが添付されないので、当該サーバ実体C_1乃至C_5には影響がない。また、仮に$ISP1_A$から正しく使用されているＨＴＴＰを使用したＤＤｏＳ攻撃が行われたとしても、ダウンするのはＨＴＴＰサービスを提供しているサーバ実体C_1だけであり、同じ代表アドレスでＦＴＰサービスを提供するサーバ実体C_4は何も影響のないまま正常にサービスを継続可能となる。

【０１３４】

また、第２実施形態と同様に、仮にサーバ実体C_1倒れたとしてもその影響範囲は$ISP1_A$のユーザだけに限定されることとなる。

【０１３５】

以上、本発明の第１乃至第３の実施形態について説明したが、本発明はこれに限定されることなく、その趣旨を逸脱しない範囲で種々の改良・変更が可能であることは勿論である。例えば、本発明は、例えば、電話音声をＩＰパケットに変換するＶｏＩＰ技術を用いて中継交換する通話システムであるＩＰ電話システムやオプティカルＶＰＮ等にも適用可能である。また、ＩＰパケットのヘッダに含まれるＴＯＳ（ｔｙｐｅ ｏｆ ｓｅｒｖｉｃｅ）に経路に関する情報を含め、当該情報に基づいて各ルータが経路制御処理を行うことによっても、同様の効果が得られる。

【０１３６】

【発明の効果】

以上詳述したように、本発明によれば、広域コンピュータネットワーク上で複数のサーバ実体を分散配置して各サーバ実体にかかる負荷を分散しつつ所定のサービスを提供するような状況下において、当該広域コンピュータネットワークを介しての外部から不正目的のアクセスがなされることによるシステム被害、例えば、ＤＤｏＳ攻撃等の被害の影響を局所化することで、情報提供サービス全体の攻撃耐性の向上と稼働率の向上とを図ることにある情報提供システム及び情報提供方法を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態に係る情報提供システムの構成を示す図である。

【図２】第１実施形態に係る情報提供システムにおいて、各サーバ実体C_1乃至C_5に対して、ユーザグループが使用する経路を決定した様子を概念的に示す図である。

【図３】第１実施形態に係る情報提供システムによる経路制御処理の流れを示すフローチャートである。

【図４】（ａ）は第１実施形態に係る情報提供システムの各ルータR_1乃至R_{10}が有する通常の経路制御処理テーブルを示す図であり、（ｂ）はサービスＳに係る転送先を定期する経路制御処理テーブルを示す図である。

【図５】第１実施形態に係る情報提供システムによる図４（ａ），（ｂ）の２つの経路制御処理テーブル参照処理を示すフローチャートである。

【図６】第１実施形態に係る情報提供システムをユーザグループG_1乃至G_5により隔離した様子を示す図である。

【図７】第２実施形態に係る情報提供システムの構成を示す図である。

【図８】第２実施形態に係る情報提供システムの構成を示す図である。

【図９】（ａ）は第２実施形態に係る情報提供システムのルータR_1が有する通常の経路制御処理テーブルを示す図であり、（ｂ）はサービスＳに係る転送先を定期する経路制御処理テーブルを示す図である。

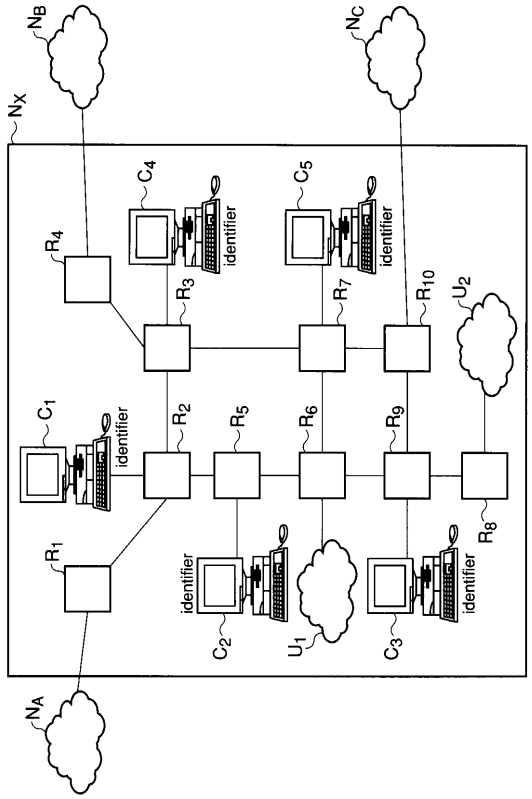
【図１０】（ａ）は第２実施形態に係る情報提供システムのルータR_2が有する通常の経路制御処理テーブルを示す図であり、（ｂ）はサービスＳに係る転送先を定期する経路制御処理テーブルを示す図である。

【図１１】第２実施形態に係る情報提供システムによるラベル情報の付加について説明するための図である。

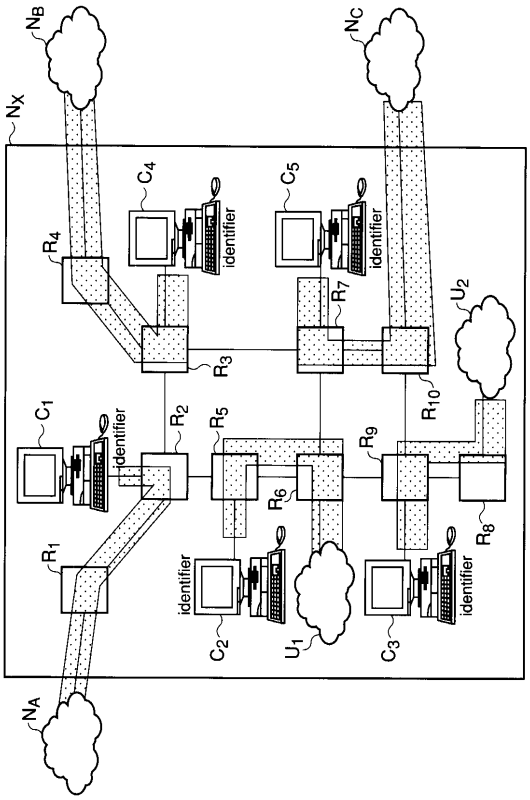
【図１２】第２実施形態に係る情報提供システムにおけるルータR_1（ＭＰＬＳエッジルータ）の経路制御テーブル参照処理について更に詳細に説明するためのフローチャートで

ある。
【図１３】第２実施形態に係る情報提供システムにおけるルータＲ２（ＭＰＬＳコアルータ）の経路制御テーブル参照処理について更に詳細に説明するためのフローチャートである。
【図１４】図８と略同様である第３実施形態に係る情報提供システムの一部拡大図である。
【図１５】（ａ）は第３実施形態に係る情報提供システムのルータR_1が有する通常の経路制御処理テーブルを示す図であり、（ｂ）はサービスＳに係る転送先を定期する経路制御処理テーブルを示す図である。
【図１６】（ａ）は第３実施形態に係る情報提供システムのルータR_2が有する通常の経路制御処理テーブルを示す図であり、（ｂ）はサービスＳに係る転送先を定期する経路制御処理テーブルを示す図である。
【図１７】（ａ）は第３実施形態に係る情報提供システムのルータR_3が有する通常の経路制御処理テーブルを示す図であり、（ｂ）はサービスＳに係る転送先を定期する経路制御処理テーブルを示す図である。
【図１８】第３実施形態に係る情報提供システムによりＣＲ－ＬＤＰを利用してラベルを配布する例を説明するための図である。
【図１９】第３実施形態に係る情報提供システムにより、サーバ実体C_4のＴＣＰ／２０にラベルが割り当てられるまでの詳細な手順を示す図である。
【図２０】（ａ）は一般的なＦＥＣ　ＴＬＶのフォーマットを示す図であり、（ｂ）は新たにタイプ０ｘ０５（タイプ：ソケット）を定義したＦＥＣ　ＴＬＶのフォーマットを示す図である。
【図２１】第３実施形態に係る情報提供システムにおけるルータR_1（ＭＰＬＳエッジルータ）の経路制御テーブル参照処理について更に詳細に説明するためのフローチャートである。
【符号の説明】
C_1～C_5　サーバ実体
R_1～R_{10}　ルータ
N_A～N_X　ネットワーク
U_1，U_2　利用ユーザ端末
G_1～G_5　ユーザグループ
T_1　通常の経路制御処理テーブル
T_2　サービスＳに関する経路制御処理テーブル

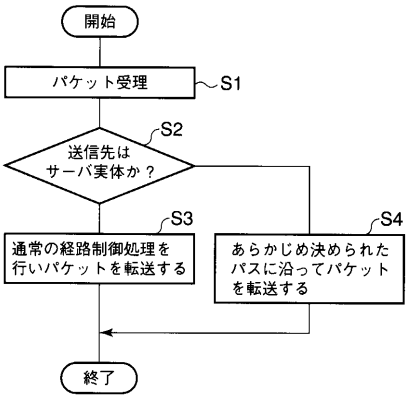
【図１】


N_B
N_C
N_X
C_4
identifier
C_5
identifier
R_4
R_3
R_7
R_{10}
U_2
C_1
identifier
R_2
R_5
R_6
R_9
R_1
R_8
identifier
identifier
C_2
U_1
C_3
identifier
N_A

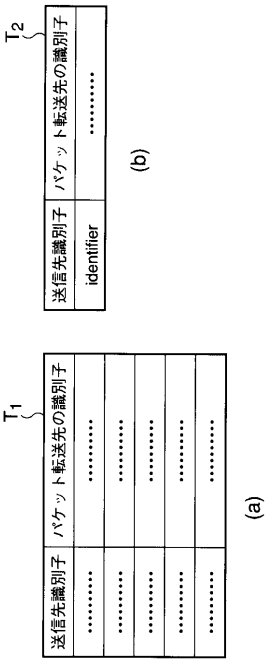
【図２】


N_B
N_C
N_X
C_4
identifier
C_5
identifier
R_4
R_3
R_7
R_{10}
U_2
C_1
identifier
R_2
R_5
R_6
R_9
R_1
R_8
identifier
identifier
C_2
U_1
C_3
identifier
N_A

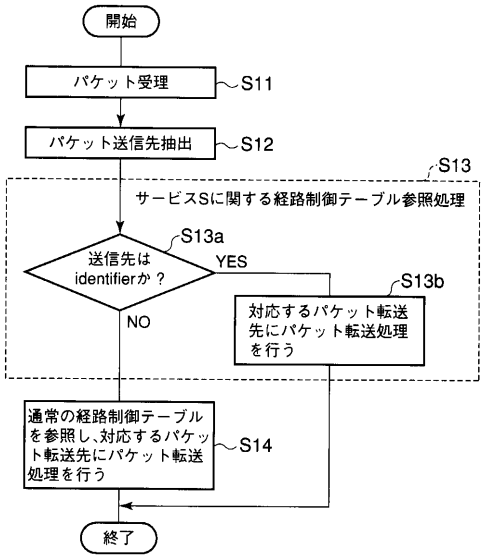
【図３】


開始
パケット受理
S1
S2
送信先は
サーバ実体か？
S3
通常の経路制御処理を
行いパケットを転送する
S4
あらかじめ決められた
パスに沿ってパケット
を転送する
終了

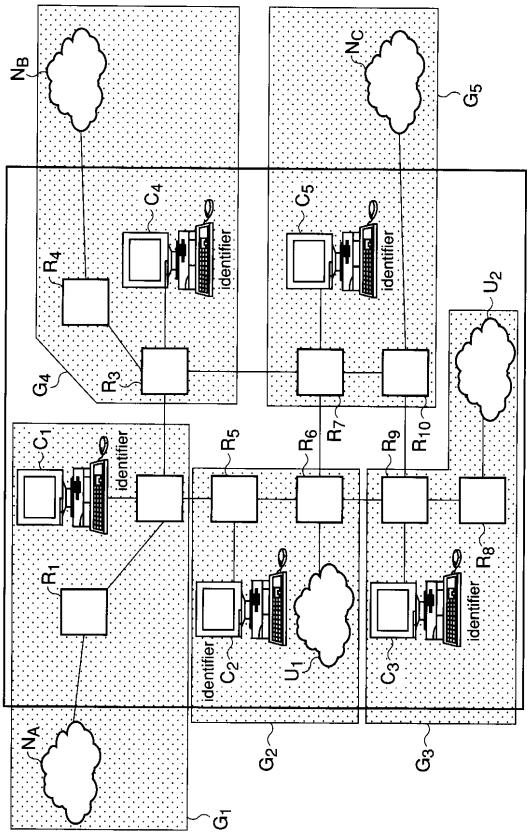
【図４】


T_2
送信先識別子
パケット転送先の識別子
identifier
(b)
T_1
送信先識別子
パケット転送先の識別子
(a)

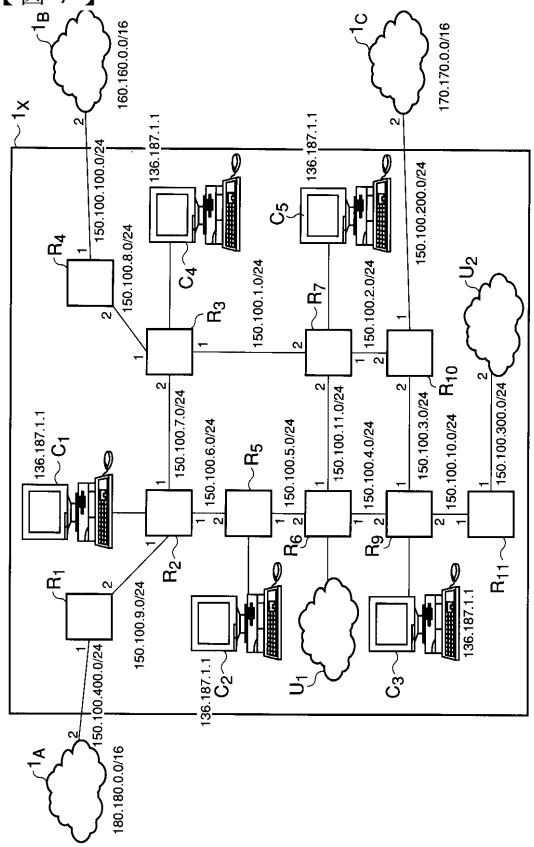
【図５】


開始
パケット受理
S11
パケット送信先抽出
S12
S13
サービスSに関する経路制御テーブル参照処理
S13a
送信先は identifierか？
YES
NO
S13b
対応するパケット転送先にパケット転送処理を行う
通常の経路制御テーブルを参照し、対応するパケット転送先にパケット転送処理を行う
S14
終了

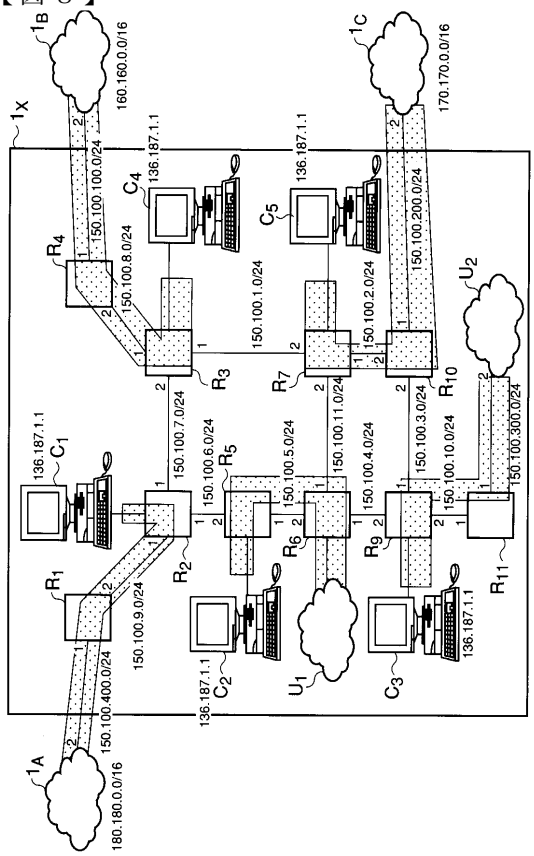
【図６】


NB
NC
G5
C4
C5
identifier
R4
R3
G4
U2
C1
R5
R6
R7
R9
R10
R8
R1
identifier
C2
U1
C3
NA
G2
G3
G1

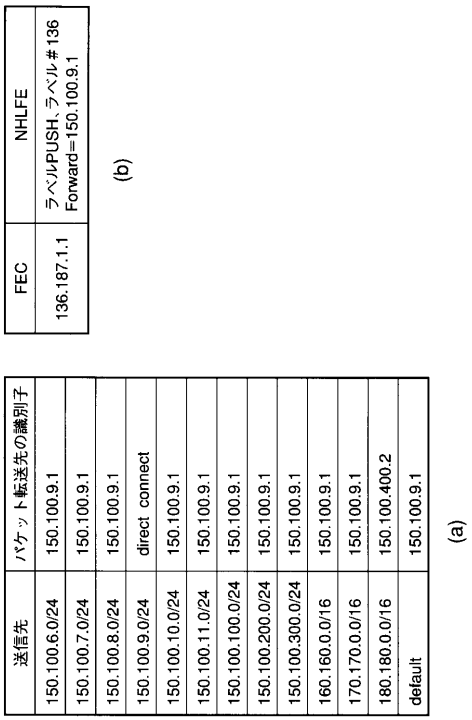
【図７】


1B
160.160.0.0/16
1C
170.170.0.0/16
1X
136.187.1.1
150.100.100.0/24
150.100.200.0/24
C4
C5
R4
R3
R7
U2
150.100.8.0/24
150.100.1.0/24
150.100.2.0/24
150.100.7.0/24
150.100.11.0/24
150.100.3.0/24
R10
150.100.300.0/24
C1
150.100.6.0/24
150.100.5.0/24
150.100.4.0/24
150.100.10.0/24
R5
R6
R9
R2
R11
R1
150.100.9.0/24
C2
U1
C3
150.100.400.0/24
1A
180.180.0.0/16

【図８】


1B
160.160.0.0/16
1C
170.170.0.0/16
1X
136.187.1.1
150.100.100.0/24
150.100.200.0/24
C4
C5
R4
R3
R7
U2
150.100.8.0/24
150.100.1.0/24
150.100.2.0/24
150.100.7.0/24
150.100.11.0/24
150.100.3.0/24
R10
150.100.300.0/24
C1
150.100.6.0/24
150.100.5.0/24
150.100.4.0/24
150.100.10.0/24
R5
R6
R9
R2
R11
R1
150.100.9.0/24
C2
U1
C3
150.100.400.0/24
1A
180.180.0.0/16

【図９】



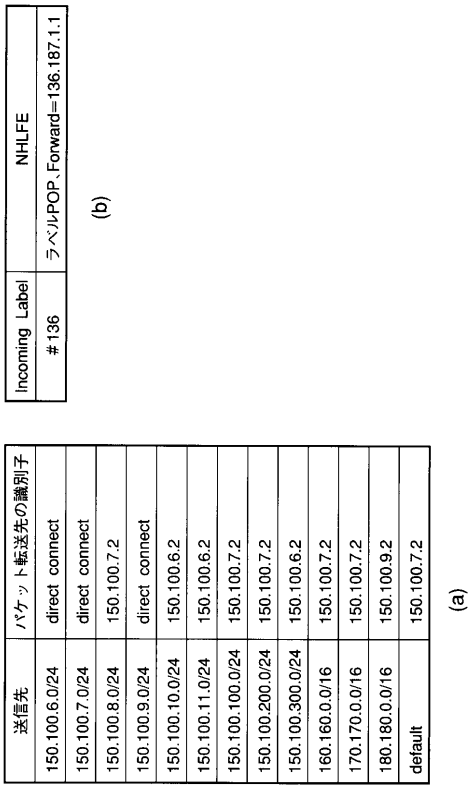
FEC	NHLFE
136.187.1.1	ラベルPUSH、ラベル＃136 Forward=150.100.9.1

(b)

送信先	パケット転送先の識別子
150.100.6.0/24	150.100.9.1
150.100.7.0/24	150.100.9.1
150.100.8.0/24	150.100.9.1
150.100.9.0/24	direct connect
150.100.10.0/24	150.100.9.1
150.100.11.0/24	150.100.9.1
150.100.100.0/24	150.100.9.1
150.100.200.0/24	150.100.9.1
150.100.300.0/24	150.100.9.1
160.160.0.0/16	150.100.9.1
170.170.0.0/16	150.100.9.1
180.180.0.0/16	150.100.400.2
default	150.100.9.1

(a)

【図１０】



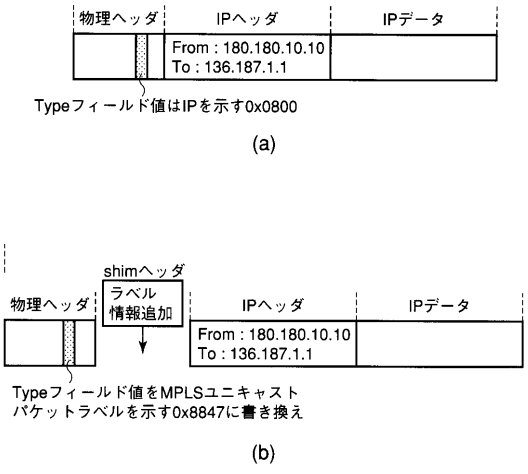
Incoming Label	NHLFE
＃136	ラベルPOP、Forward=136.187.1.1

(b)

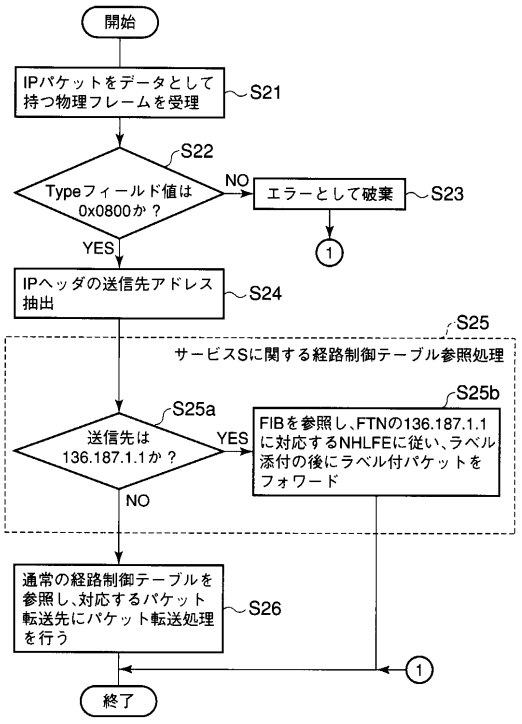
送信先	パケット転送先の識別子
150.100.6.0/24	direct connect
150.100.7.0/24	direct connect
150.100.8.0/24	150.100.7.2
150.100.9.0/24	direct connect
150.100.10.0/24	150.100.6.2
150.100.11.0/24	150.100.6.2
150.100.100.0/24	150.100.7.2
150.100.200.0/24	150.100.7.2
150.100.300.0/24	150.100.6.2
160.160.0.0/16	150.100.7.2
170.170.0.0/16	150.100.7.2
180.180.0.0/16	150.100.9.2
default	150.100.7.2

(a)

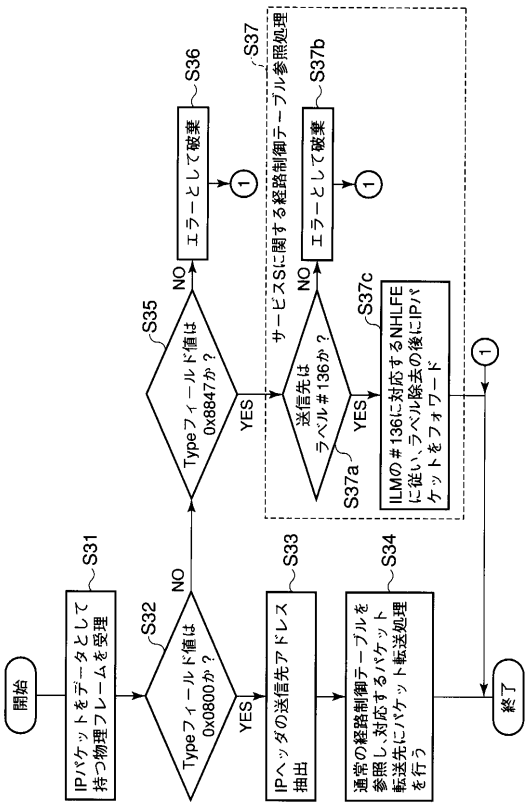
【図１１】



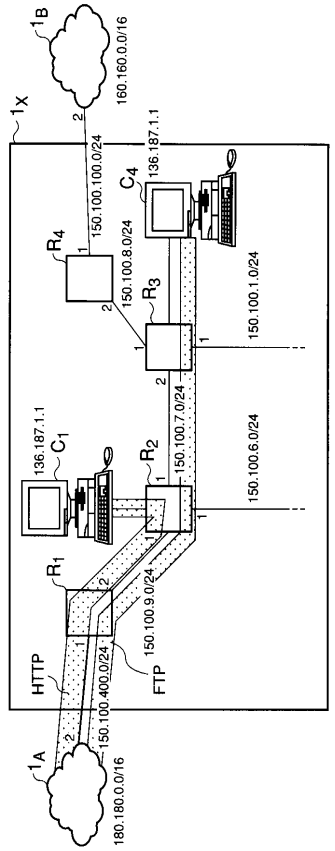
【図１２】



【図１３】



【図１４】



【図１５】

送信先	パケット転送先の識別子
150.100.6.0/24	150.100.9.1
150.100.7.0/24	150.100.9.1
150.100.8.0/24	150.100.9.1
150.100.9.0/24	direct connect
150.100.10.0/24	150.100.9.1
150.100.11.0/24	150.100.9.1
150.100.100.0/24	150.100.9.1
150.100.200.0/24	150.100.9.1
150.100.300.0/24	150.100.9.1
160.160.0.0/16	150.100.9.1
170.170.0.0/16	150.100.9.1
180.180.0.0/16	150.100.400.2
default	150.100.9.1

(a)

FEC	NHLFE
136.187.1.1,TCP/80	ラベルPUSH、ラベル＃136 Forward=150.100.9.1
136.187.1.1,TCP/20	ラベルPUSH、ラベル＃137 Forward=150.100.9.1
136.187.1.1,TCP/21	

(b)

【図１６】

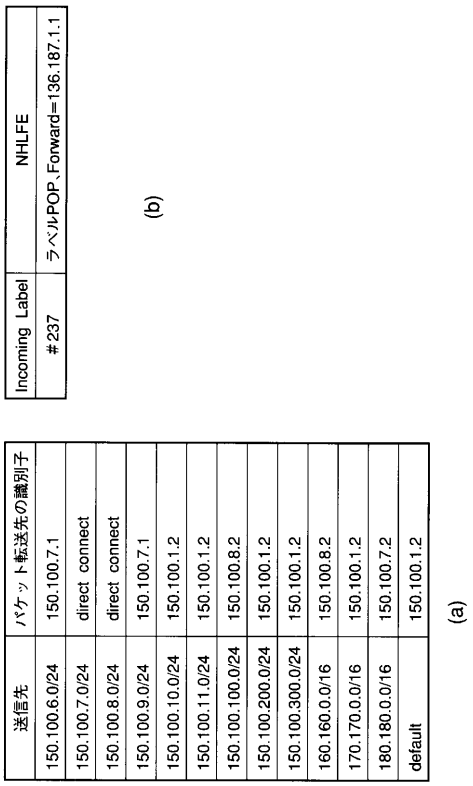
送信先	パケット転送先の識別子
150.100.6.0/24	direct connect
150.100.7.0/24	direct connect
150.100.8.0/24	150.100.7.2
150.100.9.0/24	direct connect
150.100.10.0/24	150.100.6.2
150.100.11.0/24	150.100.6.2
150.100.100.0/24	150.100.7.2
150.100.200.0/24	150.100.7.2
150.100.300.0/24	150.100.6.2
160.160.0.0/16	150.100.7.2
170.170.0.0/16	150.100.7.2
180.180.0.0/16	150.100.9.2
default	150.100.7.2

(a)

Incoming Label	NHLFE
＃136	ラベルPOP、Forward=136.187.1.1
＃137	ラベルSWAP、Newlabel=＃237, Forward=150.100.7.2

(b)

【図１７】



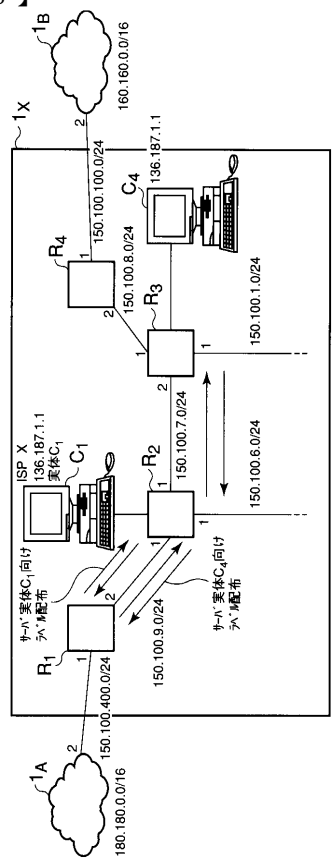
送信先	パケット転送先の識別子
150.100.6.0/24	150.100.7.1
150.100.7.0/24	direct connect
150.100.8.0/24	direct connect
150.100.9.0/24	150.100.7.1
150.100.10.0/24	150.100.1.2
150.100.11.0/24	150.100.1.2
150.100.100.0/24	150.100.8.2
150.100.200.0/24	150.100.1.2
150.100.300.0/24	150.100.1.2
160.160.0.0/16	150.100.8.2
170.170.0.0/16	150.100.1.2
180.180.0.0/16	150.100.7.2
default	150.100.1.2

(a)

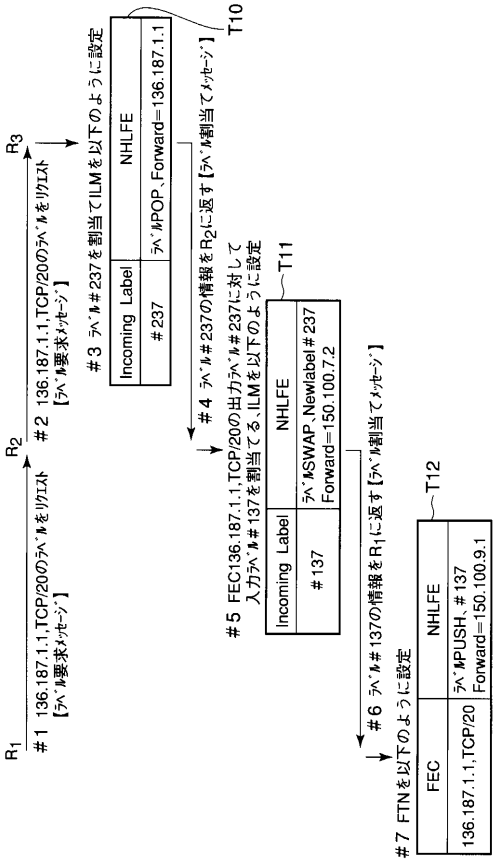
Incoming Label	NHLFE
#237	ラベルPOP、Forward=136.187.1.1

(b)

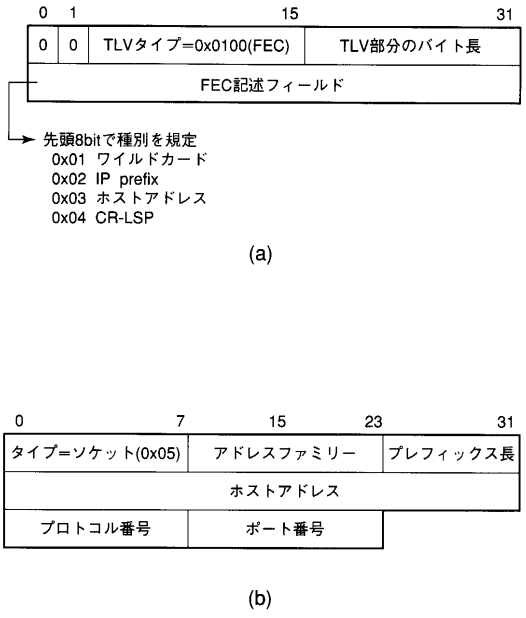
【図１８】



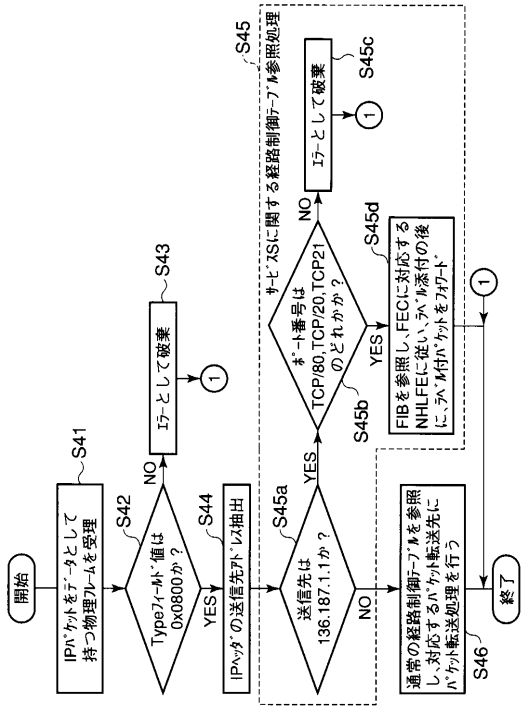
【図１９】



【図２０】



【図２１】


開始
S41
IPﾊﾟｹｯﾄをﾃﾞｰﾀとして
持つ物理ﾌﾚｰﾑを受理
S42
Typeﾌｨｰﾙﾄﾞ値は
0x0800か？
NO
S43
ｴﾗｰとして破棄
YES
S44
IPﾍｯﾀﾞの送信先ｱﾄﾞﾚｽ抽出
S45
ｻｰﾋﾞｽに関する経路制御ﾃｰﾌﾞﾙ参照処理
S45a
送信先は
136.187.1.1か？
YES
NO
S45b
ﾎﾟｰﾄ番号は
TCP/80,TCP/20,TCP21
のどれかか？
NO
S45c
ｴﾗｰとして破棄
YES
S45d
FIBを参照し、FECに対応する
NHLFEに従い、ﾗﾍﾞﾙ付加の後
にﾗﾍﾞﾙ付ﾊﾟｹｯﾄをﾌｫﾜｰﾄﾞ
通常の経路制御ﾃｰﾌﾞﾙを参照
し、対応するﾊﾟｹｯﾄ転送先に
ﾊﾟｹｯﾄ転送処理を行う
S46
終了

フロントページの続き

(71)出願人 503058795
藤野 貴之
東京都文京区水道２丁目１３番４号 ４０５号室
(71)出願人 597165744
松方 純
神奈川県川崎市幸区小倉１番地１号
(71)出願人 502306660
日本テレコム株式会社
東京都中央区八丁堀四丁目７番１号
(74)代理人 100058479
弁理士 鈴江 武彦
(74)代理人 100091351
弁理士 河野 哲
(74)代理人 100088683
弁理士 中村 誠
(74)代理人 100108855
弁理士 蔵田 昌俊
(74)代理人 100075672
弁理士 峰 隆司
(74)代理人 100109830
弁理士 福原 淑弘
(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 藤野 貴之
東京都文京区水道２丁目１３番４号 ４０５号室
(72)発明者 淺野 正一郎
東京都世田谷区桜丘三丁目２０番２３号
(72)発明者 阿部 俊二
神奈川県横浜市青葉区千草台３７番地３９ ２０３号室
(72)発明者 計 宇生
東京都練馬区田柄１丁目１８番２２号 ３１２号室
(72)発明者 趙 偉平
神奈川県横浜市栄区小菅ヶ谷１丁目５番６号 ２０１号室
(72)発明者 松方 純
神奈川県川崎市幸区小倉１番地１号 Ｂ－１１１５号室
(72)発明者 石松 宏和
東京都中央区八丁堀四丁目７番１号 日本テレコム株式会社内
(72)発明者 橋本 健
東京都中央区八丁堀四丁目７番１号 日本テレコム株式会社内
(72)発明者 田中 伸哉
東京都中央区八丁堀四丁目７番１号 日本テレコム株式会社内

Ｆターム(参考) 5B085 AA08 BA06 BG02 BG03 BG07
5K030 GA03 GA12 GA15 HA08 HC01 HC14 JA11 KA05 LB05 LD10