(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4302004号
(P4302004)
(45)発行日　平成21年7月22日(2009.7.22)　(24)登録日　平成21年5月1日(2009.5.1)

(51)Int.Cl.　F I
H04L 12/56 (2006.01)　H04L 12/56　260A
H04L 12/56　B

請求項の数 22　(全 24 頁)

(21)出願番号　特願2004-172993(P2004-172993)
(22)出願日　平成16年6月10日(2004.6.10)
(65)公開番号　特開2005-354410(P2005-354410A)
(43)公開日　平成17年12月22日(2005.12.22)
審査請求日　平成18年7月14日(2006.7.14)

(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　100102587
弁理士　渡邊　昌幸
(72)発明者　佐藤　裕昭
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　玉木　宏治

最終頁に続く

(54)【発明の名称】パケットフィルタ設定方法およびパケットフィルタ設定システム

(57)【特許請求の範囲】

【請求項１】

少なくとも１のルータとホストを有するＩＰネットワークにおいて、ルータにパケットフィルタ条件を設定するパケットフィルタ設定方法であって、

特定のＩＰマルチキャストアドレスを、パケットフィルタ条件の情報を転送する、設定要求パケット用アドレスとして定義し、

ホストは、前記設定要求パケット用アドレスを宛先ＩＰアドレスとし、パケットフィルタ条件を記述した、設定要求パケットを送信し、

ルータは、宛先ＩＰアドレスが設定要求パケット用アドレスであるパケットを受信したら、当該パケットを終端し、記述された内容を解析し、記述されたパケットフィルタ条件を、受信したインタフェースの出力側に設定することを特徴とするパケットフィルタ設定方法。

【請求項２】

少なくとも１のルータとホスト、およびパケットフィルタ条件の設定要求を認証するとともに設定変更を許可するホストを記憶する認証手段を有するＩＰネットワークにおいて、ルータにパケットフィルタ条件を設定するパケットフィルタ設定方法であって、

認証手段には、設定変更を許可するホストを予め登録しておき、

ホストは、設定要求パケットに、正当なホストであることを証明するデータを付与し、

ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータを、パケットフィルタ条件の設定要求を認証する手段に転送し、

認証手段は、設定要求パケットを送信したホストが、正当なホストであることを確認した場合には、設定許可をルータに通知し、
ルータは、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定することを特徴とするパケットフィルタ設定方法。
【請求項３】
少なくとも１のルータとホストを有するＩＰネットワークにおけるパケットフィルタ設定システムであって、
特定のＩＰマルチキャストアドレスを、パケットフィルタ条件の情報を転送する、設定要求パケット用アドレスとして定義しておき、
ホストは、前記設定要求パケット用アドレスを宛先ＩＰアドレスとし、パケットフィルタ条件を記述した、設定要求パケットを送信する機能部を有し、
ルータは、宛先ＩＰアドレスが設定要求パケット用アドレスであるパケットを受信したら、当該パケットを終端し、記述された内容を解析し、記述されたパケットフィルタ条件を、受信したインタフェースの出力側に設定する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項４】
請求項３に記載のパケットフィルタ設定システムであって、
ルータは、前記機能部に加えて、フィルタ設定が成功した場合、ホストに完了通知を送信する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項５】
請求項３または４に記載のパケットフィルタ設定システムであって、
ホストは、前記機能部に加えて、設定要求パケットを周期的に送信する機能部を有し、
ルータは、前記機能部に加えて、予め定めた一定期間以上、設定要求パケットを受信しない場合に、当該フィルタ設定を削除する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項６】
請求項３または４に記載のパケットフィルタ設定システムであって、
ＩＰネットワークにおいて、特定のＩＰマルチキャストアドレスを、パケットフィルタの確認パケット用アドレスとして定義しておき、
ルータは、予め定めた一定周期で、宛先ＩＰアドレスを確認パケット用アドレスとして、確認パケットを送信する機能部を有し、
ホストは、宛先ＩＰアドレスが確認パケット用アドレスのパケットを受信したら、設定要求パケットを送信する機能部を有し、
また、ルータは、予め定めた一定期間以上、設定要求パケットを受信しない場合に、当該フィルタ条件を削除する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項７】
少なくとも１のルータとホスト、およびパケットフィルタ条件の設定要求を認証するとともに設定変更を許可するホストを記憶する認証手段を有するパケットフィルタ設定システムであって、
認証手段には、設定変更を許可するホストを予め登録しておき、
ホストは、設定要求パケットに、正当なホストであることを証明するデータを付与して送信する機能部を有し、
ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータを、認証手段に転送する機能部を有し、
前記認証手段は、設定要求パケットを送信したホストが、正当なホストであることを確認した場合には、設定許可をルータに通知する機能部を有し、
ルータは、さらに、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定する機能部を有することを特徴とするパケットフィルタ設定システム。

【請求項８】
請求項７に記載のパケットフィルタ設定システムであって、
認証手段は、前記機能部に加えて、各ホストに対して変更を許可するパケットフィルタ条件を記憶する機能部を有し、
前記認証手段には、予め、各ホストに対して変更を許可するパケットフィルタ条件を登録しておき、
ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータに加えて、パケットフィルタ条件を、認証手段に転送する機能部を有し、
認証手段は、設定要求パケットを送信したホストが、正当なホストであり、かつ、パケットフィルタ条件が、各ホストに対して変更を許可するパケットフィルタ条件に該当することを確認した場合、設定許可をルータに通知する機能部を有し、
ルータは、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項９】
請求項８に記載のパケットフィルタ設定システムであって、
認証手段は、各ホストに対して変更を許可するパケットフィルタ条件を記憶する代わりに、各ホストに対して変更を許可しないパケットフィルタ条件を記憶する機能部を有し、
認証手段は、設定要求が、各ホストに対して変更を許可しないパケットフィルタ条件に合致しない場合に、設定許可をルータに通知する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項１０】
請求項８に記載のパケットフィルタ設定システムであって、
認証手段は、各ホストの変更を許可するパケットフィルタ条件を記憶する機能部と、各ホストに対して変更を許可しないパケットフィルタ条件を記憶する機能部の両方を有することを特徴とするパケットフィルタ設定システム。
【請求項１１】
請求項７～１０のいずれか１項に記載のパケットフィルタ設定システムであって、
ルータは、認証手段から通知された認証結果を、設定要求を送信したホストに通知する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項１２】
請求項３～１１のいずれか１項に記載のパケットフィルタ設定システムであって、
設定要求パケットに記述する内容は、動作識別子と条件記述との１以上の組み合わせから構成されており、
動作識別子は、追加と削除との２種類定義しておき、
ホストは、パケットフィルタ条件を追加する場合に、動作識別子が追加で、追加条件を記述した設定要求を送信する、あるいは、パケットフィルタ条件を削除する場合に、動作識別子が削除で、削除条件を記述した設定要求を送信する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項１３】
請求項３～１１のいずれか１項に記載のパケットフィルタ設定システムであって、
設定要求パケットに記述する内容は、動作識別子と条件記述との１以上の組み合わせから構成され、動作識別子は追加／削除識別子と転送／遮断識別子とから構成されており、
ホストは、遮断条件を追加する場合に、追加／削除識別子が追加で、転送／遮断識別子が遮断で、追加する遮断条件を記述した条件設定パケットを送信する、
あるいは、転送条件を追加する場合に、追加／削除識別子が追加で、転送／遮断識別子が転送で、追加する転送条件を記述した条件設定パケットを送信する、
あるいは、遮断条件を削除する場合に、追加／削除識別子が削除で、転送／遮断識別子が遮断で、削除する遮断条件を記述した条件設定パケットを送信する、
あるいは、転送条件を削除する場合に、追加／削除識別子が削除で、転送／遮断識別子

が転送で、削除する転送条件を記述した条件設定パケットを送信する機能部を有することを特徴とするパケットフィルタ設定システム。

【請求項１４】

請求項３～１１のいずれか１項に記載のパケットフィルタ設定システムであって、

設定要求パケットに記述する内容は、動作識別子と条件記述との１以上の組み合わせから構成され、動作識別子は、遮断条件追加，転送条件追加，遮断条件削除，転送条件削除の４種類を定義しておき、

ホストは、遮断条件を追加する場合に、動作識別子が遮断条件追加で、追加する遮断条件を記載した条件設定パケットを送信する、

あるいは、転送条件を追加する場合に、動作識別子が転送条件追加で、追加する転送条件を記載した条件設定パケットを送信する、

あるいは、遮断条件を削除する場合に、動作識別子が遮断条件削除で、削除する遮断条件を記載した条件設定パケットを送信する、

あるいは、転送条件を削除する場合に、動作識別子が転送条件削除で、削除する転送条件を記載した条件設定パケットを送信する機能部を有することを特徴とするパケットフィルタ設定システム。

【請求項１５】

請求項３～１４のいずれか１項に記載のパケットフィルタ設定システムであって、

ルータの出力インタフェースのパケットフィルタ条件の初期状態は、当該ルータ発パケットを除き全遮断としておき、

ルータは、転送条件のみを追加および削除する機能部を有することを特徴とするパケットフィルタ設定システム。

【請求項１６】

請求項３～１４のいずれか１項に記載のパケットフィルタ設定システムであって、

ルータのインタフェースのパケットフィルタ条件の初期状態を、全て転送としておき、

ルータは、遮断条件のみを追加および削除する機能部を有することを特徴とするパケットフィルタ設定システム。

【請求項１７】

請求項３～１５のいずれか１項に記載のパケットフィルタ設定システムであって、

ルータのインタフェースは、送信元アドレスのみの条件指定で、ある送信元アドレスに対して、少なくとも１のホストが要求するパケットフィルタ条件が転送である場合に、ルータは、当該送信元アドレスのパケットを転送設定する機能部を有するものであることを特徴とするパケットフィルタ設定システム。

【請求項１８】

請求項３～１４，１６のいずれか１項に記載のパケットフィルタ設定システムであって、

ルータのインタフェースにおいて、送信元アドレスのみの条件指定で、ある送信元アドレスに対して、全てのホストが要求するパケットフィルタ条件が、遮断である場合に限り、ルータは、当該送信元アドレスのパケットを遮断設定する機能部を有するものであることを特徴とするパケットフィルタ設定システム。

【請求項１９】

請求項１６に記載のパケットフィルタ設定システムであって、

ルータは、遮断を要求する設定要求を受信した場合に、全ノードマルチキャストアドレスに対して、当該遮断条件を記述した遮断確認パケットを送信する機能部を有し、

遮断確認パケットを受信したホストは、転送を希望する場合は、当該条件に対して転送設定要求を送信する機能部を有し、

ルータは、さらに、転送設定要求を受信した場合は、転送条件のまま変更せず、あるいは、予め定めた時間内に転送設定要求を受信しない場合には、遮断設定する機能部を有することを特徴とするパケットフィルタ設定システム。

【請求項２０】

請求項３～１５，１７のいずれか１項に記載のパケットフィルタ設定システムであって、
パケットフィルタ設定を行ったルータは、１以上のインタフェースにおいて、ある送信元アドレスに対し、フィルタ条件が送信元アドレス限定で、かつ転送であれば、当該送信元アドレスへの選択ルートであるインタフェースから、当該転送条件を記述した設定要求パケットを送信する機能部を有し、
当該転送条件を記述した設定要求パケットを受信した隣接ルータは、受信インタフェースに、当該条件を設定する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項２１】
請求項３～１４，１６，１８，１９のいずれか１項に記載のパケットフィルタ設定システムであって、
パケットフィルタ設定を行ったルータは、ある送信元アドレスに対し、どのインタフェースにも転送設定がなければ、当該送信元アドレスへの選択ルートであるインタフェースから、当該送信元アドレスに対する遮断条件を記述した設定要求パケットを送信する機能部を有し、
当該遮断条件を記述した設定要求パケットを受信した隣接ルータは、受信インタフェースに、当該遮断条件を設定する機能部を有することを特徴とするパケットフィルタ設定システム。
【請求項２２】
請求項３～２１のいずれか１項に記載のパケットフィルタ設定システムを実現するためのルータまたはホストの機能部の機能を、コンピュータのプログラム制御により実行するための、コンピュータ制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＩＰネットワークのルータにおいて、パケットの転送、あるいは遮断を実施するフィルタリング技術に関し、より具体的には、パケットフィルタ設定方法、並びにこれを具体化したパケットフィルタ設定システムに関するものである。
【背景技術】
【０００２】
周知のように、パケットフィルタリングは、パケットのあて先アドレス、あるいは送信元アドレスとあて先アドレスの組み合わせを調べて、通過させて良いパケットと、阻止すべきパケットとを区別することであり、これにより、余分なトラフィックが生じないように抑制するとともに、セキュリティ機能を実現するための簡便な方法である。
【０００３】
従来のパケットフィルタ設定方法としては、特許文献１に示されているように、ＣＯＰＳ（Common Open Policy Service ）プロトコルや、ＳＮＭＰ（Simple Network Management Protocol ）を用いて、ネットワーク管理者の管理に基づき、ポリシーの１つとしてフィルタ条件を設定する方法が考えられている。
【０００４】
【特許文献１】特開２００３－１７３３０１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
しかしながら、上記の従来方法では、ネットワーク管理者がネットワークを制御するための手段であって、ホストが自身のセキュリティ制御のためにルータにリアルタイムにフィルタ条件を設定変更することはできないという問題がある。従って、ルータに接続しているホストが、フィルタ設定を行いたい場合には、自らのホストに設定するか、ネットワーク管理者に依頼してルータに設定してもらう必要があり、リアルタイムな変更は行うこ

とができない。

【０００６】

例えば、ファイル転送が必要な時のみftp（File Transfer Protocol ）を使用可能とし、それ以外の場合は、セキュリティの観点からftpによる接続を遮断する場合や、ネットワークの導通確認が必要な時のみ、icmp（Internet Control Message Protocol ）パケットを到達可能とする場合には、ホストにおいてフィルタ制御しなければならず、ルータ・ホスト間で無効なパケットが転送されるとともに、ホストのフィルタリング処理が行われＣＰＵ能力を消費する。

【０００７】

本発明の目的は、上記従来技術に基づく問題点を解消し、受信側が必要としないパケットが送信元に近いルータで遮断され、無効なパケット転送がなくなるようにして、回線を有効活用可能とするパケットフィルタ設定方法、並びにこれを実現するためのパケットフィルタ設定システムを提供することにある。

【課題を解決するための手段】

【０００８】

上記目的を達成するために、本発明の請求項１に記載のパケットフィルタ設定方法は、少なくとも１のルータとホストを有するＩＰネットワークにおいて、ルータにパケットフィルタ条件を設定するパケットフィルタ設定方法であって、特定のＩＰマルチキャストアドレスを、パケットフィルタ条件の情報を転送する、設定要求パケット用アドレスとして定義し、ホストは、前記設定要求パケット用アドレスを宛先ＩＰアドレスとし、パケットフィルタ条件を記述した、設定要求パケットを送信し、ルータは、宛先ＩＰアドレスが設定要求パケット用アドレスであるパケットを受信したら、当該パケットを終端し、記述された内容を解析し、記述されたパケットフィルタ条件を、受信したインタフェースの出力側に設定することを特徴とする。

本請求項に係るパケットフィルタ設定方法によれば、ホストがホスト方向のパケットフィルタを設定でき、自分に対する攻撃があった場合に、瞬時に対応することができるという効果がある。

【０００９】

本発明の請求項２に記載のパケットフィルタ設定方法は、少なくとも１のルータとホスト、およびパケットフィルタ条件の設定要求を認証するとともに設定変更を許可するホストを記憶する認証手段を有するＩＰネットワークにおいて、ルータにパケットフィルタ条件を設定するパケットフィルタ設定方法であって、認証手段には、設定変更を許可するホストを予め登録しておき、ホストは、設定要求パケットに、正当なホストであることを証明するデータを付与し、ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータを、設定要求を認証する手段に転送し、認証手段は、設定要求パケットを送信したホストが、正当なホストであることを確認した場合には、設定許可をルータに通知し、ルータは、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定することを特徴とする。

本請求項に係るパケットフィルタ設定方法によれば、悪意のユーザがルータにフィルタを設定することを防止できるという効果が得られる。

【００１０】

一方、本発明の請求項３に記載のパケットフィルタ設定システムは、少なくとも１のルータとホストを有するＩＰネットワークにおけるパケットフィルタ設定システムであって、特定のＩＰマルチキャストアドレスを、パケットフィルタ条件の情報を転送する、設定要求パケット用アドレスとして定義しておき、ホストは、前記設定要求パケット用アドレスを宛先ＩＰアドレスとし、パケットフィルタ条件を記述した、設定要求パケットを送信する機能部を有し、ルータは、宛先ＩＰアドレスが設定要求パケット用アドレスであるパケットを受信したら、当該パケットを終端し、記述された内容を解析し、記述されたパケットフィルタ条件を、受信したインタフェースの出力側に設定する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ホストがホスト方向のパケットフィルタを設定でき、自分に対する攻撃があった場合に、瞬時に対応することができるという効果がある。

【００１１】

本発明の請求項４に記載のパケットフィルタ設定システムは、請求項３に記載のパケットフィルタ設定システムであって、ルータは、前記機能部に加えて、フィルタ設定が成功した場合、ホストに完了通知を送信する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ホストは、フィルタが設定できたか否かを確認できるという効果が得られる。

【００１２】

本発明の請求項５に記載のパケットフィルタ設定システムは、請求項３または４に記載のパケットフィルタ設定システムであって、ホストは、前記機能部に加えて、設定要求パケットを周期的に送信する機能部を有し、ルータは、前記機能部に加えて、予め定めた一定期間以上、設定要求パケットを受信しない場合に、当該フィルタ設定を削除する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータは、フィルタが有効なものか、既に不要なものかを確認することができるという効果が得られる。

【００１３】

本発明の請求項６に記載のパケットフィルタ設定システムは、請求項３または４に記載のパケットフィルタ設定システムであって、ＩＰネットワークにおいて、特定のＩＰマルチキャストアドレスを、パケットフィルタの確認パケット用アドレスとして定義しておき、ルータは、予め定めた一定周期で、宛先ＩＰアドレスを確認パケット用アドレスとして、確認パケットを送信する機能部を有し、ホストは、宛先ＩＰアドレスが確認パケット用アドレスのパケットを受信したら、設定要求パケットを送信する機能部を有し、また、ルータは、予め定めた一定期間以上、設定要求パケットを受信しない場合に、当該フィルタ条件を削除する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータは、フィルタが有効なものか、既に不要なものかを確認することができるとともに、確認作業に対する処理負荷を調整することができるという効果が得られる。

【００１４】

本発明の請求項７に記載のパケットフィルタ設定システムは、少なくとも１のルータとホスト、およびパケットフィルタ条件の設定要求を認証するとともに設定変更を許可するホストを記憶する認証手段を有するパケットフィルタ設定システムであって、認証手段には、設定変更を許可するホストを予め登録しておき、ホストは、設定要求パケットに、正当なホストであることを証明するデータを付与して送信する機能部を有し、ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータを、認証手段に転送する機能部を有し、前記認証手段は、設定要求パケットを送信したホストが、正当なホストであることを確認した場合には、設定許可をルータに通知する機能部を有し、ルータは、さらに、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、悪意のユーザがルータにフィルタを設定することを防止できるという効果が得られる。

【００１５】

本発明の請求項８に記載のパケットフィルタ設定システムは、請求項７に記載のパケットフィルタ設定システムであって、前記認証手段は、前記機能部に加えて、各ホストに対して変更を許可するパケットフィルタ条件を記憶する機能部を有し、前記認証手段には、予め、各ホストに対して変更を許可するパケットフィルタ条件を登録しておき、ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータに加えて、パケットフィルタ条件を、認証手段に転送する機能部を有し、認証手段は、設定要求パケットを送信したホストが、正当なホストであり、かつ、パケットフィルタ条件が、各ホス

トに対して変更を許可するパケットフィルタ条件に該当することを確認した場合、設定許可をルータに通知する機能部を有し、ルータは、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータは、悪意のあるフィルタ条件を無断で設定することを防止することができるという効果が得られる。

【００１６】

本発明の請求項９に記載のパケットフィルタ設定システムは、請求項８に記載のパケットフィルタ設定システムであって、認証手段は、各ホストに対して変更を許可するパケットフィルタ条件を記憶する代わりに、各ホストに対して変更を許可しないパケットフィルタ条件を記憶する機能部を有し、認証手段は、設定要求が、各ホストに対して変更を許可しないパケットフィルタ条件に合致しない場合に、設定許可をルータに通知する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータは、悪意のあるフィルタ条件を無断で設定することを防止することができるという効果が得られる。

【００１７】

本発明の請求項１０に記載のパケットフィルタ設定システムは、請求項８に記載のパケットフィルタ設定システムであって、認証手段は、各ホストの変更を許可するパケットフィルタ条件を記憶する機能部と、各ホストに対して変更を許可しないパケットフィルタ条件を記憶する機能部の両方を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータは、悪意のあるフィルタ条件を無断で設定することを防止することができるとともに、ホストが意図するフィルタ条件を作成しやすくなるという効果が得られる。

【００１８】

本発明の請求項１１に記載のパケットフィルタ設定システムは、請求項７～１０のいずれか１項に記載のパケットフィルタ設定システムであって、ルータは、認証手段から通知された認証結果を、設定要求を送信したホストに通知する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ホストは、認証が成功したか失敗したかを確認することができるという効果が得られる。

【００１９】

本発明の請求項１２に記載のパケットフィルタ設定システムは、請求項３～１１のいずれか１項に記載のパケットフィルタ設定システムであって、設定要求パケットに記述する内容は、動作識別子と条件記述との１以上の組み合わせから構成されており、動作識別子は、追加と削除との２種類定義しておき、ホストは、パケットフィルタ条件を追加する場合に、動作識別子が追加で、追加条件を記述した設定要求を送信する、あるいは、パケットフィルタ条件を削除する場合に、動作識別子が削除で、削除条件を記述した設定要求を送信する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータにおける処理が容易になるという効果が得られる。

【００２０】

本発明の請求項１３に記載のパケットフィルタ設定システムは、請求項３～１１のいずれか１項に記載のパケットフィルタ設定システムであって、設定要求パケットに記述する内容は、動作識別子と条件記述との１以上の組み合わせから構成され、動作識別子は追加／削除識別子と転送／遮断識別子とから構成されており、ホストは、遮断条件を追加する場合に、追加／削除識別子が追加で、転送／遮断識別子が遮断で、追加する遮断条件を記述した条件設定パケットを送信する、あるいは、転送条件を追加する場合に、追加／削除識別子が追加で、転送／遮断識別子が転送で、追加する転送条件を記述した条件設定パケットを送信する、あるいは、遮断条件を削除する場合に、追加／削除識別子が削除で、転送／遮断識別子が遮断で、削除する遮断条件を記述した条件設定パケットを送信する、あ

るいは、転送条件を削除する場合に、追加／削除識別子が削除で、転送／遮断識別子が転送で、削除する転送条件を記述した条件設定パケットを送信する機能部を有することを特徴とする。

なお、本明細書中において記号「／」は、「または」を意味している。

本請求項に係るパケットフィルタ設定システムによれば、ルータにおける処理が容易になるという効果が得られる。

【００２１】

本発明の請求項１４に記載のパケットフィルタ設定システムは、請求項３～１１のいずれか１項に記載のパケットフィルタ設定システムであって、設定要求パケットに記述する内容は、動作識別子と条件記述との１以上の組み合わせから構成され、動作識別子は、遮断条件追加，転送条件追加，遮断条件削除，転送条件削除の４種類を定義しておき、ホストは、遮断条件を追加する場合に、動作識別子が遮断条件追加で、追加する遮断条件を記載した条件設定パケットを送信する、あるいは、転送条件を追加する場合に、動作識別子が転送条件追加で、追加する転送条件を記載した条件設定パケットを送信する、あるいは、遮断条件を削除する場合に、動作識別子が遮断条件削除で、削除する遮断条件を記載した条件設定パケットを送信する、あるいは、転送条件を削除する場合に、動作識別子が転送条件削除で、削除する転送条件を記載した条件設定パケットを送信する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ルータにおける処理が容易になるという効果が得られる。

【００２２】

本発明の請求項１５に記載のパケットフィルタ設定システムは、請求項３～１４のいずれか１項に記載のパケットフィルタ設定システムであって、ルータの出力インタフェースのパケットフィルタ条件の初期状態は、当該ルータ発パケットを除き全遮断としておき、ルータは、転送条件のみを追加および削除する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ホストにとって安全側の制御を行うことができるという効果が得られる。

【００２３】

本発明の請求項１６に記載のパケットフィルタ設定システムは、請求項３～１４のいずれか１項に記載のパケットフィルタ設定システムであって、ルータのインタフェースのパケットフィルタ条件の初期状態を、全て転送としておき、ルータは、遮断条件のみを追加および削除する機能部を有することを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、ホストにとって通信ができないというトラブルを減少させることが可能になるという効果が得られる。

【００２４】

本発明の請求項１７に記載のパケットフィルタ設定システムは、請求項３～１５のいずれか１項に記載のパケットフィルタ設定システムであって、ルータのインタフェースは、送信元アドレスのみの条件指定で、ある送信元アドレスに対して、少なくとも１のホストが要求するパケットフィルタ条件が転送である場合に、ルータは、当該送信元アドレスのパケットを転送設定する機能部を有するものであることを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、シェアードメディアにおいて、あるホストの受信拒否が他のホストに影響を与えないという効果が得られる。

【００２５】

本発明の請求項１８に記載のパケットフィルタ設定システムは、請求項３～１４，１６のいずれか１項に記載のパケットフィルタ設定システムであって、ルータのインタフェースにおいて、送信元アドレスのみの条件指定で、ある送信元アドレスに対して、全てのホストが要求するパケットフィルタ条件が、遮断である場合に限り、ルータは、当該送信元アドレスのパケットを遮断設定する機能部を有するものであることを特徴とする。

本請求項に係るパケットフィルタ設定システムによれば、シェアードメディアにおいて、あるホストの受信拒否が他のホストに影響を与えないという効果が得られる。

【００２６】
本発明の請求項１９に記載のパケットフィルタ設定システムは、請求項１６に記載のパケットフィルタ設定システムであって、ルータは、遮断を要求する設定要求を受信した場合に、全ノードマルチキャストアドレスに対して、当該遮断条件を記述した遮断確認パケットを送信する機能部を有し、遮断確認パケットを受信したホストは、転送を希望する場合は、当該条件に対して転送設定要求を送信する機能部を有し、ルータは、さらに、転送設定要求を受信した場合は、転送条件のまま変更せず、あるいは、予め定めた時間内に転送設定要求を受信しない場合には、遮断設定する機能部を有することを特徴とする。
本請求項に係るパケットフィルタ設定システムによれば、シェアードメディアにおいて、あるパケットに対し必要なホストと不要なホストと不要なホストが混在する場合、両者の要望に合わせたフィルタ条件を作成できるという効果が得られる。
【００２７】
本発明の請求項２０に記載のパケットフィルタ設定システムは、請求項３～１５，１７のいずれか１項に記載のパケットフィルタ設定システムであって、パケットフィルタ設定を行ったルータは、１以上のインタフェースにおいて、ある送信元アドレスに対し、フィルタ条件が送信元アドレス限定で、かつ転送であれば、当該送信元アドレスへの選択ルートであるインタフェースから、当該転送条件を記述した設定要求パケットを送信する機能部を有し、当該転送条件を記述した設定要求パケットを受信した隣接ルータは、受信インタフェースに、当該条件を設定する機能部を有することを特徴とする。
本請求項に係るパケットフィルタ設定システムによれば、送信元に近いルータでパケット遮断を行うことが可能になるという効果が得られる。
【００２８】
本発明の請求項２１に記載のパケットフィルタ設定システムは、請求項３～１４，１６，１８，１９のいずれか１項に記載のパケットフィルタ設定システムであって、パケットフィルタ設定を行ったルータは、ある送信元アドレスに対し、どのインタフェースにも転送設定がなければ、当該送信元アドレスへの選択ルートであるインタフェースから、当該送信元アドレスに対する遮断条件を記述した設定要求パケットを送信する機能部を有し、当該遮断条件を記述した設定要求パケットを受信した隣接ルータは、受信インタフェースに、当該遮断条件を設定する機能部を有することを特徴とする。
本請求項に係るパケットフィルタ設定システムによれば、送信元に近いルータでパケット遮断を行うことが可能になるという効果が得られる。
【００２９】
また、本発明は、請求項２２に記載の通り、上記各項に記載のパケットフィルタ設定システムを実現するためのルータまたはホストの機能部の機能を、コンピュータのプログラム制御により実行するための、コンピュータ制御プログラムをも提供するものである。
【００３０】
特に、本発明は、請求項３～２１のいずれか１項に記載のパケットフィルタ設定システムを構成するに好適に用い得るルータを提供することをも、その特徴とする。すなわち、請求項３～２１のいずれか１項に記載のパケットフィルタ設定システムは、その特徴的機能を実現するルータによるところが大きい。
【００３１】
以上をまとめると、本発明においては、ホストがセキュリティ用にルータからホスト方向へのパケット転送に限定して、フィルタ条件を設定する。この場合、リアルタイムにフィルタ条件の変更を可能とするように、ＩＰパケットにフィルタ条件を記述しネットワークレイヤで制御する。また、ルータがフィルタ条件の設定パケットかどうかを容易に判断することができるように、予め定めたＩＰマルチキャストアドレスを用いる。
【００３２】
また、本発明に係る技術においては、ホストは事前にルータに通知せず電源断や回線断が発生する可能性が大きいため、ルータが周期的に監視することにより、フィルタ条件の有効性を確認することは有効である。また、ネットワークセキュリティの観点から、ルー

タに不正なフィルタ条件を設定されないように、設定要求をネットワークで認証することも有効である。

【００３３】

また、上記の設定要求の認証においては、認証サーバにフィルタ条件のうちの変更可能な条件，変更不可能な条件あるいは条件範囲を記憶し、認証条件で参照することにより、セキュリティを向上させることができる。

また、認証結果をホストに通知することにより、ホストでネットワークの動作を確認することが可能になる。

【００３４】

ルータにおけるフィルタ条件設定においては、設定処理が追加であるか削除であるか、あるいは遮断条件であるか転送条件であるかをを識別子として明示的に指定することが、ルータにおける、条件記述解析の高速化や処理負荷の低減に有効である。

また、ルータの初期条件を、全て遮断か全て転送かに定めておけば、条件追加処理が簡略化される。

【００３５】

また、通常、ルータのインタフェースには、一般的に複数のホストが接続されることが考えられ、その場合には、各ホストから要望されるフィルタ条件の論理和を取った条件を設定する必要がある。特に遮断の要求がある場合には、要求元以外に遮断しても良いかを問い合わせることにより、突然パケットを受信しなくなる故障が発生した場合との区別が容易になる。

【００３６】

また、ルータのフィルタ条件を、上流ルータのフィルタ条件に反映させれば、上流ルータ間の回線に無効パケットが転送されることがなくなり、回線が有効活用できる。

【発明の効果】

【００３７】

本発明によれば、ＩＰネットワークにおいて、受信側が必要としないパケットが送信元に近いルータで遮断され、無効なパケット転送がなくなるという効果が得られる。なお、本発明のより具体的な効果は、下記の実施例により詳細に示される。

【発明を実施するための最良の形態】

【００３８】

以下に、添付の図面に示す好適実施形態に基づいて、を詳細に説明する。

【００３９】

〔実施例１〕

本発明の実施例１を、図１のネットワーク構成例を用いて説明する。

ルータ１０１とホスト１０２，ホスト１０３，ホスト１０４から構成される。

ルータ１０１には、ホスト１０２を接続するインタフェース（１）（以下、インタフェースをＩＦと、インタフェース（１）をＩＦ（１）等と略記する）１１１と、ホスト１０３およびホスト１０４が接続されるＩＦ（２）１１２が存在する。ホスト１０２のＩＰアドレスを2002::2とし、ホスト１０３のＩＰアドレスを3000::2とし、ホスト１０４のＩＰアドレスを4000::2とする。また、フィルタ条件設定パケット用のＩＰアドレスを、例えば、ff02::100と定めておく。

上記のネットワーク構成例やＩＰアドレスの値は、説明を明確化するための一例であって、本発明を制限するものではない。

【００４０】

実施例１の動作を、図２の動作例を用いて説明する。

ホスト１０２は、ホスト１０３からのパケット受信を拒否する場合に、送信元3000::2のパケットを遮断と記述し、宛先ＩＰアドレスをff02::100としたフィルタ設定要求パケットを送信する（Ｓ１，Ｓ２）。

ルータ１０１は、ＩＦ（１）１１１にて、宛先ＩＰアドレスがff02::100であるフィルタ設定要求パケットを受信したら、記述内容を解析し（Ｓ３）、送信元3000::2を遮断と

記述されているので、当該パケットを受信したＩＦ（１）１１１の出力方向に、3000::2からのパケットを遮断するフィルタを設定する（Ｓ４）。

【００４１】

あるいは、ホスト１０２はホスト１０３からのパケット受信を拒否する場合に、送信元3000::2、宛先2000::2のパケットを遮断と記述し、宛先ＩＰアドレスをff02::100としたフィルタ設定要求パケットを送信する方法もある。

その場合、ルータ１０１はＩＦ（１）１１１にて、宛先ＩＰアドレスがff02::100であるフィルタ設定要求パケットを受信したら、記述内容を解析し、送信元3000::2，宛先2000::2のパケットを遮断と記述されているので、当該パケットを受信したＩＦ（１）１１１の出力方法に、送信元3000::2，宛先2000::2のパケットを遮断するフィルタを設定する。

【００４２】

〔実施例２〕

本発明の実施例２のネットワーク構成は、図１と同様である。

本発明の実施例２の動作を、図３の動作例を用いて説明する。

実施例２では、ルータ１０１がＩＦ（１）１１１の出力方向に、3000::2からのパケットを遮断するフィルタを設定後（Ｓ５～Ｓ７）に、ホスト１０２にフィルタ設定完了通知を送信する（Ｓ８）ところが実施例１と異なる。

【００４３】

〔実施例３〕

本発明の実施例３のネットワーク構成例は、図１と同様である。

本発明の実施例３の動作例は、図４に示すように、ホスト１０２が周期的にフィルタ設定通知を送信する（Ｓ１０～Ｓ１２）ところ、およびルータ１０１がフィルタ設定時にタイマを起動する（Ｓ１４）ところが異なる。

ルータ１０１は、タイマ動作中にフィルタ設定通知を受信したら、タイマを更新する（Ｓ１５）。

あるいは、ルータ１０１はフィルタ設定通知を、ある一定時間以上受信せずタイムアウトしたら、設定したフィルタ条件を解除する（Ｓ１６～Ｓ１７）。

【００４４】

〔実施例４〕

本発明の実施例４の動作例を、図５に示す。図５に示すように、ルータがフィルタ設定を確認し、フィルタ設定通知はフィルタ設定確認の応答として送信されるところが、実施例３と異なる。

ルータ１０１は、確認送信タイマを用いて、フィルタ設定確認通知を周期的に送信する（Ｓ２２～Ｓ２７）。フィルタ設定確認通知の宛先アドレスは、実施例１のフィルタ条件設定パケット用のＩＰアドレスと同一で、パケットの記述内容で識別してもよいし、異なるＩＰアドレスとし、ＩＰアドレスにより識別してもよい。

フィルタ条件継続タイマの動作は、実施例３のタイマ動作と同様である。

【００４５】

〔実施例５〕

本発明の実施例５のネットワーク構成を、図６に示す。実施例５のネットワーク構成は、図１に示す実施例１のネットワーク構成に、認証サーバ２０５を追加した構成である。すなわち、ルータ２０１とホスト２０２，ホスト２０３，ホスト２０４および認証サーバ２０５から構成される。

ルータ２０１にはホスト２０２を接続するＩＦ（１）２１１と、ホスト２０３および２０４が接続されるＩＦ（２）２１２が存在する。また、ホスト２０２のＩＰアドレスを2000::2とし、ホスト２０３のＩＰアドレスを3000::2とし、ホスト２０４のＩＰアドレスを4000::2とする。

【００４６】

実施例５の動作を、図７の動作例を用いて説明する。

実施例５では、ホストはフィルタ設定要求にホスト認証情報を添付する。ホスト情報と

しては、ユーザＩＤとパスワードの組み合わせ，電子証明書などが考えられるが、本発明は、ルータにおいてホストから受信したフィルタ設定要求と、その認証結果を対応付けできることが重要であって、ホスト認証方法を限定するものではない。

ルータ２０１はフィルタ設定要求を受信したら、当該メッセージに添付されたホスト認証情報を認証サーバ２０５に転送し（Ｓ２９～Ｓ３１）、その応答を受信した時に応答が認証成功であればフィルタ設定を実行する（Ｓ３２～Ｓ３４）。

なお、図8に示すように、認証サーバ２０５からの応答が認証失敗であれば、ルータ２０１はフィルタ設定を実行しない（Ｓ３５～Ｓ３８）。

【００４７】

〔実施例６〕

本発明の実施例６のネットワーク構成および動作は、実施例５と同様である。

ただし、認証サーバ２０５にホストが変更してもよいフィルタ条件を登録しておく点と、ルータ２０１が認証サーバ２０５に送信する認証要求に、ホスト認証情報だけでなく、フィルタ条件をも添付する所が異なる。図９に、認証サーバの２０５のフィルタ条件管理テーブル構成例を示す。

フィルタ条件管理テーブルは、ホスト名と変更許可範囲とから構成される。ホスト名は、図９では、ホストのＩＰアドレスを例として示すが、ホストを識別できればよく、他にもＭＡＣアドレスでも、文字列からなるユーザＩＤでもよい。変更範囲は、図９では、ＩＰアドレスの１つの範囲を例として示すが、ＩＰアドレス，ＩＰプロトコル番号，ＴＣＰポート番号，ＵＤＰポート番号，ＩＣＭＰタイプ，コードの組み合わせを複数記述してもよい。

【００４８】

各ホストが設定可能なフィルタ条件は、上記のように、認証サーバ２０５に予め登録しておき、認証サーバ２０５は、ルータ２０１から通知されたフィルタ条件が、登録してあるフィルタ条件の範囲内であれば、認証成功通知に、当該フィルタ条件を添付し、ルータ２０１は認証成功に添付されたフィルタ条件を設定する。

あるいは、認証サーバ２０５は、実施例５と異なり、ホストが認証されても、当該ホストからの設定変更要求条件が変更範囲になければ、認証失敗をルータに応答することも考えられる。図９のテーブル記述例でいえば、認証サーバ２０５は、ホスト2002::2から送信元ＩＰ＝3000::2の遮断要求を許可されるが、同ホストの送信元ＩＰ＝4000::2の遮断要求は拒否する。

【００４９】

〔実施例７〕

本発明の実施例７のネットワーク構成および動作は、実施例６と同様である。

ただし、認証サーバ２０５に、ホストが変更できないフィルタ条件を登録しておく点が実施例６と異なる。この場合、認証サーバ２０５は、ホストからの設定変更要求条件が変更不可範囲になければ、認証成功通知にホストから要求されたフィルタ条件を添付し、ルータ２０１は、認証成功に添付されたフィルタ条件を設定する。また、認証サーバ２０５は、ホストからの設定変更要求条件が変更不可範囲にあれば、認証失敗をルータ２０１に応答することも考えられる。

【００５０】

〔実施例８〕

本発明の実施例８のネットワーク構成および動作は、実施例６と同様である。

ただし、認証サーバ２０５に、ホストが変更してもよいフィルタ条件と、ホストが変更できないフィルタ条件の両方を登録しておく点が、実施例６と異なる。

この場合、認証サーバ２０５の動作としては、フィルタ条件管理テーブルに一括して変更してもよい条件と変更できない条件を記憶する方法でも、あるいは変更してもよい条件のテーブルと変更できない条件のテーブルをそれぞれ用意し、両方を参照する方法でもよい。

認証サーバ２０５のフィルタ条件管理テーブル検索動作例としては、予めフィルタ条件

を登録順、あるいは優先度順に整列記憶させ、検索時には最初に合致した条件を適用する方法や、あるいは、フィルタ条件登録時に各フィルタ条件の優先度を明記してフィルタ条件管理テーブルに記憶し、フィルタ条件管理テーブル検索時には、合致した条件のうち優先度が最高の条件を適用する方法が考えられる。

【００５１】

〔実施例９〕

本発明の実施例９の動作を、図１０と図１１の動作例を用いて説明する。

図１０の動作例１は、認証成功時の動作を示し、ルータ２０１は認証サーバ２０５から認証成功を通知された場合に、ホストに認証成功を通知する（Ｓ４１～Ｓ４４）。認証成功は、実施例２の設定完了通知が兼ねてもよい。また、図１１の動作例は、認証失敗時の動作を示し、ルータ２０１は認証サーバ２０５から認証失敗を通知された場合に、ホストに認証失敗を通知する（Ｓ４７～Ｓ４９）。

また、予めルータ２０１に送信回数を設定し、ルータ２０１は認証成功通知および認証失敗通知を設定した回数送信することも考えられる。

【００５２】

〔実施例１０〕

本発明の実施例１０の設定要求パケットフォーマット例を、図１２に示す。

設定要求パケットは、ＩＰヘッダとデータとから構成される。ＩＰヘッダには、図のようにＩＰオプションヘッダが追加される場合がある。データは条件毎に複数記述可能で、各データは、動作識別子とデータ長と条件内容とから構成される。動作識別子は、例えば追加が１で、削除は２とする。追加と削除が識別できれば、他の値でもよい。

転送か遮断かの識別は、条件内容に含まれる。

【００５３】

〔実施例１１〕

本発明の実施例１１の設定要求パケットフォーマット例を、図１３に示す。

設定要求パケットは、実施例１０の図１２と基本部分は同様であるが、動作識別子が、追加／削除識別子と、転送／遮断識別子であるところが異なる。追加／削除識別子は、例えば、追加が１で削除は２とする。追加と削除が識別できれば他の値でもよい。転送／遮断識別子は、例えば転送が１で遮断が２とする。転送と遮断が識別できれば他の値でもよい。実施例１１では、実施例１０と異なり、転送か遮断が明示的に示されているため、条件内容に転送か遮断かは含まれない。

【００５４】

〔実施例１２〕

本発明の実施例１２の設定要求パケットフォーマット例は、図１２と同様である。

ただし、動作識別子の定義が異なる。動作識別子は、例えば遮断条件追加が１で、転送条件追加は２、遮断条件削除が３、転送条件削除が４とする。もちろん、上記４種類が識別できれば、他の値でもよい。

実施例１２では、実施例１０と異なり、転送か遮断が明示的に示されているため、条件内容に転送か遮断かは含まれない。

【００５５】

〔実施例１３〕

本発明の実施例１３の動作を、図１４の動作例を用いて説明する。

初期状態にて、ルータ２０１のホスト２０２接続ＩＦ（１）２１１では、ルータ発を除き、全ての出力を遮断している（Ｓ５０）。

例えば、ホスト２０２は送信元ＩＰアドレスが3000::2の遮断条件の設定要求を送信しても、元々遮断なので処理は実施されない（Ｓ５１，Ｓ５２）。次に、上記アドレスの転送条件を設定した場合、ルータ２０１において転送設定される（Ｓ５３～Ｓ５５）。この時、ルータ２０１が設定完了通知，認証成功通知，認証失敗通知を送信する場合には、ルータ発のパケットは遮断の対象外なので、送信される。

【００５６】

〔実施例１４〕
本発明の実施例１４の動作を、図１５の動作例を用いて説明する。
初期状態にて、ルータ２０１のホスト２０２接続ＩＦ（１）２１１では、ルータ２０１発を除き、全ての出力を転送設定している（Ｓ５６）。
例えば、ホスト２０２は送信元ＩＰアドレスが3000::2の転送条件の設定要求を送信しても、元々転送なので、処理は実施されない（Ｓ５７，Ｓ５８）。次に、上記アドレスの遮断条件を設定した場合、ルータ２０１において遮断設定される（Ｓ５９～Ｓ６１）。
【００５７】
〔実施例１５〕
本発明の実施例１５のシステム構成例を図１６、動作例を図１７に示す。
ここでは、ルータ３０１のＩＦ（１）３１１にＩＰアドレスが2000::2のホスト３０２から2000::4のホスト３０４までの３台のホストが接続されている構成で説明する。
実施例１５の動作は、図１７に例示するように、ホスト３０２が3000::2からのパケットを遮断要求した場合、ルータ３０１のＩＦ（１）３１１には遮断設定される（Ｓ６２，Ｓ６３）。次に、ホスト３０３が3000::2からのパケットを転送要求した場合、同一インタフェースであるＩＦ（１）３１１に接続されるホストの一つが転送であるため、ＩＦ（１）３１１としては、転送設定となる（Ｓ６４，Ｓ６５）。
次に、ホスト３０４が3000::2からのパケットを遮断要求した場合、同一インタフェースであるＩＦ（１）３１１に接続されるホストの一つが転送であるため、転送設定のままで条件変更はされない（Ｓ６６，Ｓ６７）。
【００５８】
〔実施例１６〕
本発明の実施例１６のネットワーク構成は図１６と同様で、ルータのＩＦ（１）３１１にＩＰアドレスが2000::2から2000::4までの３台のホストが接続されている構成で説明する。
実施例１６の動作は、図１８に示すように、ＩＰアドレス3000::2のホスト３０５が転送設定であるとする（Ｓ６８）。ホスト３０２が3000::2からのパケットを遮断要求した場合、他のホストは遮断でないために条件変更はしない（Ｓ６９，Ｓ７０）。次に、ホスト３０３が3000::2からのパケットを遮断要求した場合にも、ホスト３０４が遮断でないため、条件変更はしない（Ｓ７１，Ｓ７２）。次に、ホスト３０４が3000::2からのパケットを遮断要求した場合、全てのホストが遮断条件となるため、3000::2からのパケットを遮断設定する（Ｓ７３，Ｓ７４）。
【００５９】
〔実施例１７〕
本発明の実施例１７のネットワーク構成は、図１６と同様で、ルータのＩＦ（１）３１１にＩＰアドレスが2000::2から2000::4までの３台のホストが接続されている構成で説明する。
実施例１７の動作例は、図１９に示すように、3000::2が転送設定であるとする（Ｓ７５）。ホスト３０２が3000::2からのパケットを遮断要求した場合（Ｓ７６）、ルータ３０１は他のホストに転送する必要があるかどうかを、遮断条件を記載した変更確認を全ノードに送信するとともに、応答監視タイマを起動する（Ｓ７７，Ｓ７８）。ルータ３０１は監視タイマがタイムアウトしたら（Ｓ７９）、3000::2からのパケットの転送が必要なホストがないと判断し、当該条件について遮断設定を行う（Ｓ８０）。
【００６０】
〔実施例１８〕
本発明の実施例１８のネットワーク構成を図２０に、動作例を図２１に示す。
実施例１８の説明に用いるネットワーク構成では、ルータ４０１にはＩＰアドレスが2001::2のホスト４０２と2002::2のホスト４０３が、それぞれＩＦ（１１）４１１とＩＦ（１２）４１２に接続されており、ＩＦ（１３）４１３にはルータ４０２のＩＦ（２１）４２１が接続され、ルータ４０２のＩＦ（２２）４２２には、それぞれＩＰアドレスが3000

::2のホスト４０６と4000::2のホスト４０７が接続されている。

【００６１】

次に、実施例１８の動作を、図２１の動作例を用いて説明する。

ルータ（１）４０１がホスト４０２からの送信元アドレスが3000::2であるパケットを転送する設定要求をＩＦ（１１）４１１にて受信した場合、ＩＦ（１１）４１１に当該転送設定を行う（Ｓ８２，Ｓ８３）。ルータ４０１において、１以上のＩＦにおいて送信元アドレスが3000::2であるパケットの転送設定がなされたので、ルータ４０１はルーチングテーブルを参照して、3000::2の選択経路であるルータ（２）４０２に、送信元アドレスが3000::2であるパケットを転送する設定要求を送信する（Ｓ８５）。

ルータ（２）４０２は、送信元アドレスが3000::2であるパケットを転送する設定要求を、ＩＦ（２１）４２１にて受信した場合、ＩＦ（２１）４２１に当該転送設定を実施する（Ｓ８６）。

【００６２】

〔実施例１９〕

本発明の実施例１９のネットワーク構成は、図２０と同様である。

以下、実施例１９の動作を、図２２の動作例を用いて説明する。

ルータ（１）４０１がホスト４０２からの送信元アドレスが3000::2であるパケットを遮断する設定要求をインタフェース４１１にて受信した場合、ＩＦ（１１）４１１に当該遮断設定を行う（Ｓ８８，Ｓ８９）。この時、ＩＦ（１２）４１２でも送信元アドレスが3000::2であるパケットが遮断設定であるとする。

【００６３】

ルータ（１）４０１では、全ＩＦにおいて、送信元アドレスが3000::2であるパケットの遮断要求設定がされたので、ルータ（１）４０１はルーチングテーブルを参照し、3000::2の選択経路であるルータ（２）４０２に送信元アドレスが3000::2であるパケットを遮断する設定要求を送信する（Ｓ９１）。ルータ（２）４０２は、送信元アドレスが3000::2であるパケットを遮断する設定要求をＩＦ（２１）４２１にて受信した場合、ＩＦ（２１）４２１に当該遮断設定を実施する（Ｓ９２）。

【００６４】

なお、前述のように、本発明に係るパケットフィルタ設定システムを実現するためのルータまたはホストの機能を、コンピュータのプログラム制御により実行するための、コンピュータ制御プログラムとしても商品化できるという効果もある。

【００６５】

また、前述のように、本発明に係るパケットフィルタ設定システムは、これを構成するために好適に用いうるルータ単体としても、商品化可能である。

例えば、以下の通りである。

（１）請求項３に記載のパケットフィルタ設定システムに用いられ、

宛先ＩＰアドレスが設定要求パケット用アドレスであるパケットを受信したら、当該パケットを終端し、記述された内容を解析し、記述されたパケットフィルタ条件を、受信したインタフェースの出力側に設定する機能部を有することを特徴とするルータ。

（２）請求項４に記載のパケットフィルタ設定システムに用いられ、

フィルタ設定が成功した場合、ホストに完了通知を送信する機能部を有することを特徴とするルータ。

（３）請求項５に記載のパケットフィルタ設定システムに用いられ、

予め定めた一定期間以上、設定要求パケットを受信しない場合に、当該フィルタ設定を削除する機能部を有することを特徴とするルータ。

【００６６】

（４）請求項６に記載のパケットフィルタ設定システムに用いられ、

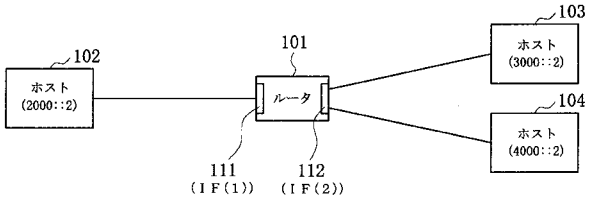
予め定めた一定周期で、宛先ＩＰアドレスを確認パケット用アドレスとして、確認パケットを送信する機能部と、

予め定めた一定期間以上、設定要求パケットを受信しない場合に、当該フィルタ条件を

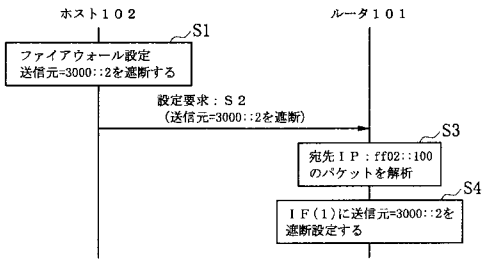
削除する機能部を有することを特徴とするルータ。
（５）請求項７に記載のパケットフィルタ設定システムに用いられ、
設定要求パケットを受信したら、正当なホストであることを証明するデータを、認証手段に転送する機能部と、
認証手段から、設定許可を通知された場合のみ、パケットフィルタ条件を、設定要求パケットを受信したインタフェースに設定する機能部を有することを特徴とするルータ。
【００６７】
（６）請求項８に記載のパケットフィルタ設定システムに用いられ、
ルータは、設定要求パケットを受信したら、正当なホストであることを証明するデータに加えて、パケットフィルタ条件を、認証手段に転送する機能部を有することを特徴とするルータ。
（７）請求項１１に記載のパケットフィルタ設定システムに用いられ、
認証手段から通知された認証結果を、設定要求を送信したホストに通知する機能部を有することを特徴とするルータ。
（８）請求項１２に記載のパケットフィルタ設定システムに用いられ、
動作識別子が追加で、追加条件を記述した設定要求を受信した場合、パケットフィルタ条件を追加し、及び、動作識別子が削除で、削除条件を記述した設定要求を受信した場合、パケットフィルタ条件を削除する場合に、機能部を有することを特徴とするルータ。
【００６８】
（９）請求項１３に記載のパケットフィルタ設定システムに用いられ、
追加削除識別子が追加で、転送遮断識別子が遮断で、追加する遮断条件を記述した条件設定パケットを受信した場合、当該遮断条件を追加し、
あるいは、追加削除識別子が追加で、転送遮断識別子が転送で、追加する転送条件を記述した条件設定パケットを受信した場合、当該転送条件を追加し、
あるいは、追加削除識別子が削除で、転送遮断識別子が遮断で、削除する遮断条件を記述した条件設定パケットを受信した場合、遮断条件を削除し、
あるいは、追加削除識別子が削除で、転送遮断識別子が転送で、削除する転送条件を記述した条件設定パケットを受信した場合、転送条件を削除する、機能部を有することを特徴とするルータ。
【００６９】
なお、上記実施形態並びに実施例は、いずれも本発明の一例を示したものであり、本発明はこれらに限定されるものではなく、本発明の趣旨を変更しない範囲内で適宜の変更・改良を行ってもよいことはいうまでもない。
【図面の簡単な説明】
【００７０】
【図１】本発明の実施例１のネットワーク構成例を示すブロック図である。
【図２】本発明の実施例１の動作例を示すシーケンス図である。
【図３】本発明の実施例２の動作例を示すシーケンス図である。
【図４】本発明の実施例３の動作例を示すシーケンス図である。
【図５】本発明の実施例４の動作例を示すシーケンス図である。
【図６】本発明の実施例５のネットワーク構成例を示すブロック図である。
【図７】本発明の実施例５の動作例１を示すシーケンス図である。
【図８】本発明の実施例５の動作例２を示すシーケンス図である。
【図９】本発明の実施例６における配信サーバのフィルタ条件管理テーブル構成例を示す図である。
【図１０】本発明の実施例９の動作例１を示すシーケンス図である。
【図１１】本発明の実施例９の動作例２を示すシーケンス図である。
【図１２】本発明の実施例１０におけるパケットフォーマット例を示す図である。
【図１３】本発明の実施例１１におけるパケットフォーマット例を示す図である。
【図１４】本発明の実施例１３の動作例を示すシーケンス図である。

【図１５】本発明の実施例１４の動作例を示すシーケンス図である。
【図１６】本発明の実施例１５のネットワーク構成例を示すブロック図である。
【図１７】本発明の実施例１５の動作例を示すシーケンス図である。
【図１８】本発明の実施例１６の動作例を示すシーケンス図である。
【図１９】本発明の実施例１７の動作例を示すシーケンス図である。
【図２０】本発明の実施例１８のネットワーク構成例を示すブロック図である。
【図２１】本発明の実施例１８の動作例を示すシーケンス図である。
【図２２】本発明の実施例１９の動作例を示すシーケンス図である。
【符号の説明】
【００７１】
　１０１，２０１，３０１，４０１，４０４　ルータ
　１０２，１０３，１０４，２０２，２０３，２０４，３０２，３０３，３０４，３０５，３０６，４０２，４０３，４０６，４０７　ホスト
　２０５　認証サーバ
　１１１，１１２，２１１，２１２，３１１，３１２，４１１，４１２，４１３，４２１　ＩＦ
　Ｓ１～Ｓ９２　処理ステップ

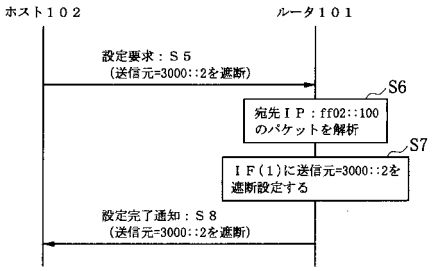
【図１】



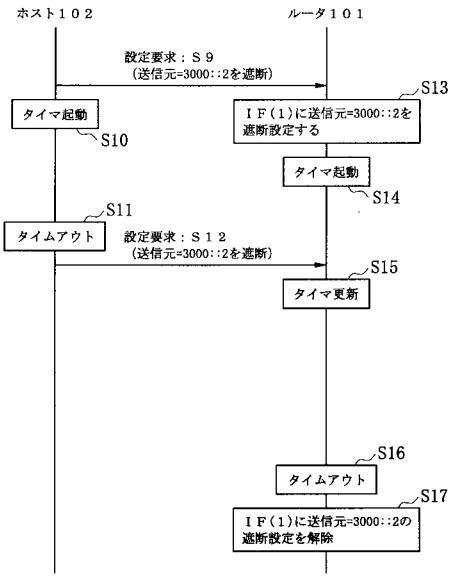
【図２】



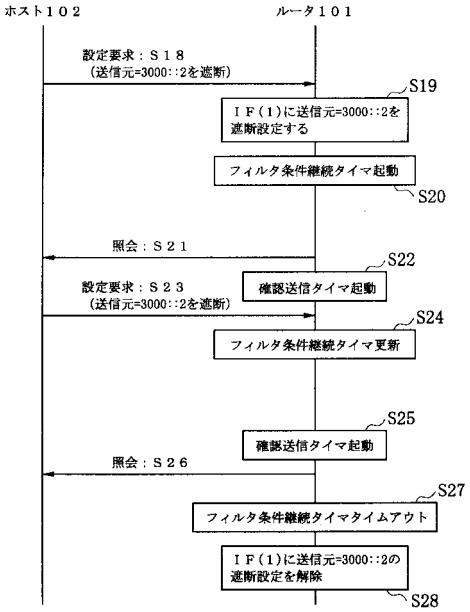
【図３】



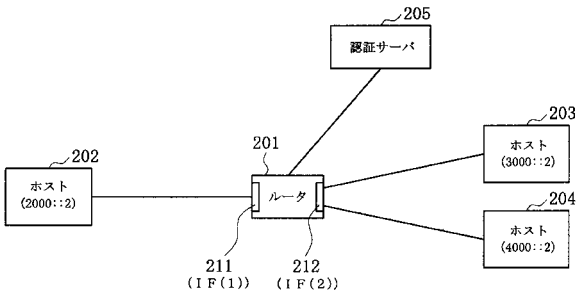
【図４】


ホスト１０２
ルータ１０１
設定要求：Ｓ９
（送信元=3000::2を遮断）
S13
タイマ起動
S10
ＩＦ(1)に送信元=3000::2を
遮断設定する
タイマ起動
S14
S11
タイムアウト
設定要求：Ｓ１２
（送信元=3000::2を遮断）
S15
タイマ更新
S16
タイムアウト
S17
ＩＦ(1)に送信元=3000::2の
遮断設定を解除

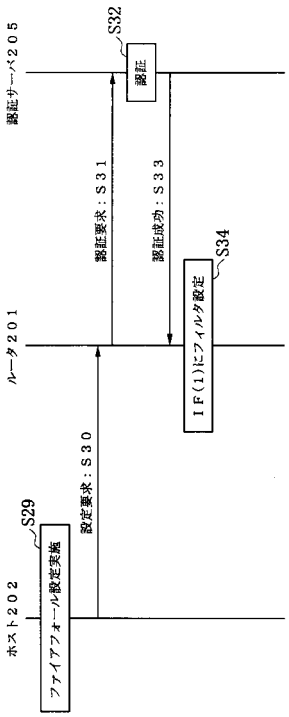
【図５】


ホスト１０２
ルータ１０１
設定要求：Ｓ１８
（送信元=3000::2を遮断）
S19
ＩＦ(1)に送信元=3000::2を
遮断設定する
フィルタ条件継続タイマ起動
S20
照会：Ｓ２１
S22
設定要求：Ｓ２３
（送信元=3000::2を遮断）
確認送信タイマ起動
S24
フィルタ条件継続タイマ更新
S25
確認送信タイマ起動
照会：Ｓ２６
S27
フィルタ条件継続タイマタイムアウト
ＩＦ(1)に送信元=3000::2の
遮断設定を解除
S28

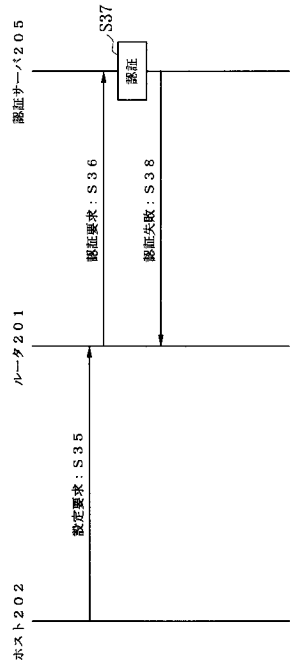
【図６】


205
認証サーバ
203
ホスト
(3000::2)
201
202
ホスト
(2000::2)
ルータ
204
ホスト
(4000::2)
211
(ＩＦ(1))
212
(ＩＦ(2))

【図７】


認証サーバ２０５
S32
認証
認証要求：Ｓ３１
認証成功：Ｓ３３
S34
ＩＦ(1)にフィルタ設定
ルータ２０１
設定要求：Ｓ３０
S29
ファイアフォール設定実施
ホスト２０２

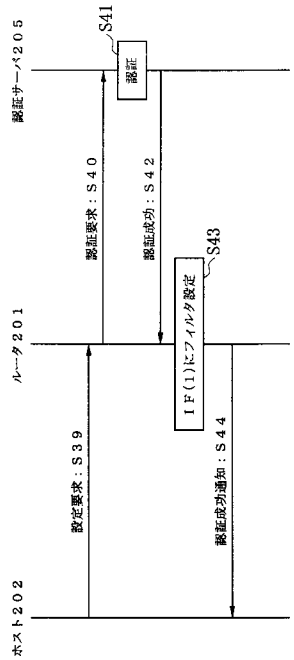
【図８】



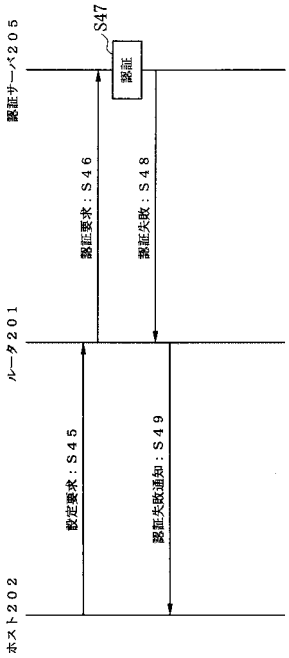
【図９】

ホスト名	変更許可範囲
2002::2	送信元ＩＰ=3000::1～3000::ffff

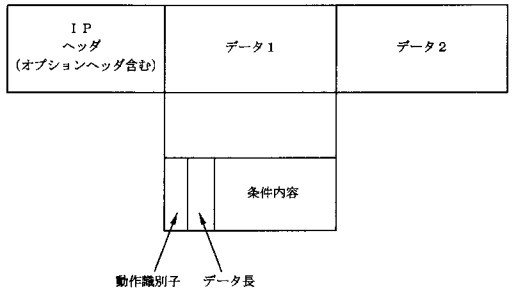
【図１０】



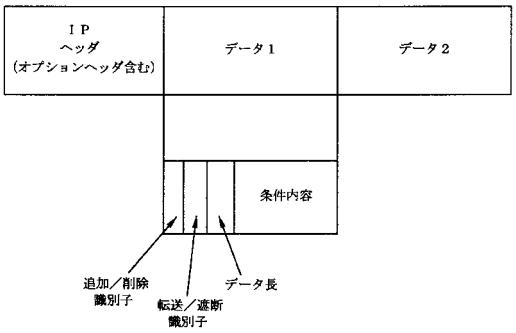
【図１１】



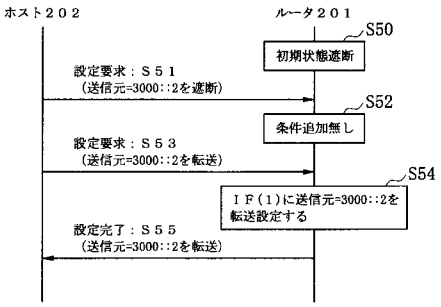
【図１２】



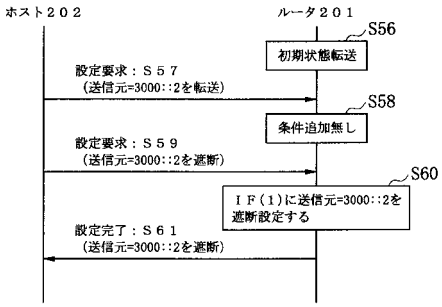
【図１３】



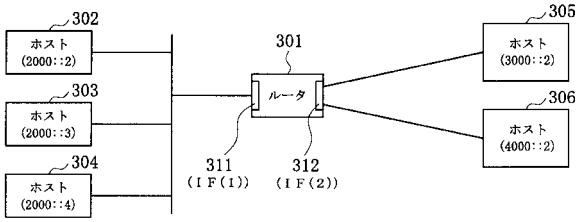
【図１４】



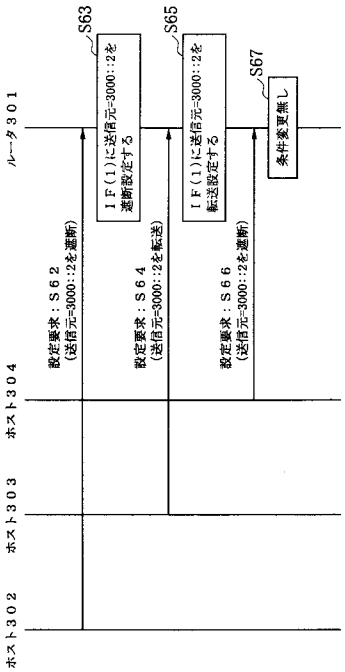
【図１５】



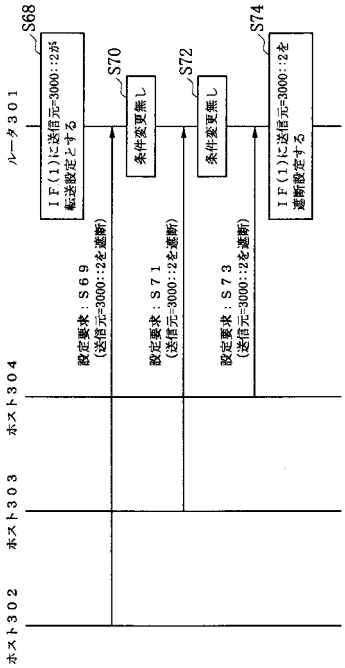
【図１６】



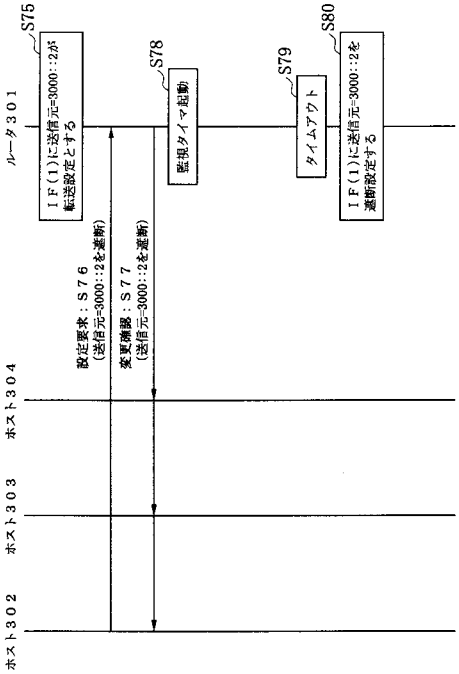
【図１７】



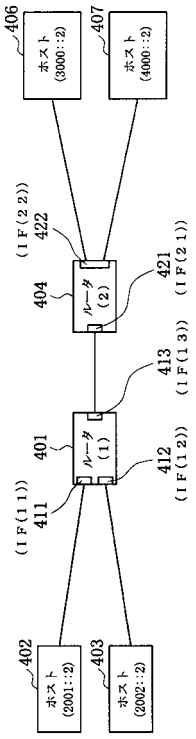
【図１８】



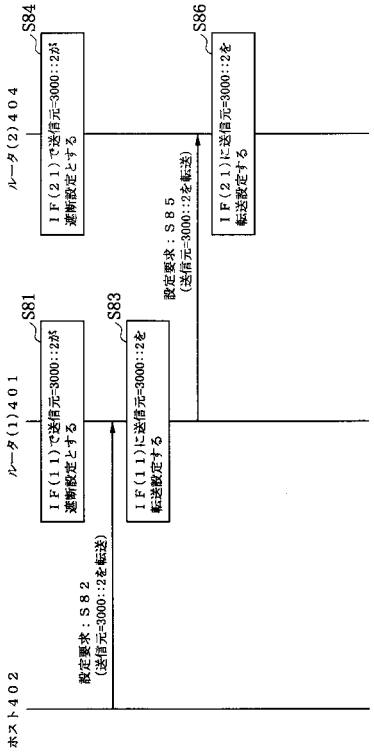
【図１９】



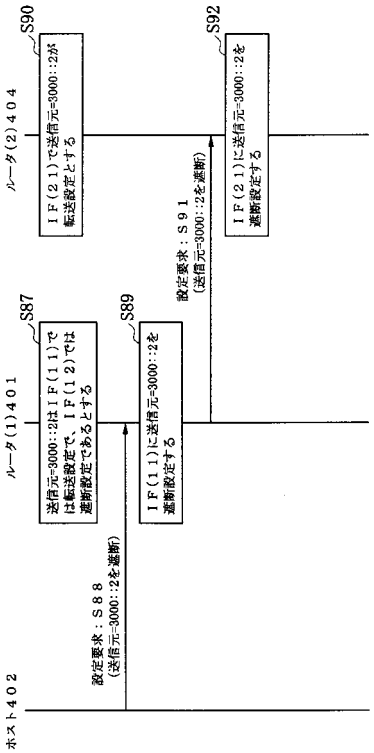
【図２０】



【図２１】


ホスト402
ルータ(1)401
ルータ(2)404
S81
IF(11)で送信元=3000::2が遮断設定とする
S82
設定要求：S82
(送信元=3000::2を転送)
S83
IF(11)に送信元=3000::2を転送設定する
S84
IF(21)で送信元=3000::2が遮断設定とする
S85
設定要求：S85
(送信元=3000::2を転送)
S86
IF(21)に送信元=3000::2を転送設定する

【図２２】


ホスト402
ルータ(1)401
ルータ(2)404
S87
送信元=3000::2はIF(11)では転送設定で、IF(12)では遮断設定であるとする
S88
設定要求：S88
(送信元=3000::2を遮断)
S89
IF(11)に送信元=3000::2を遮断設定する
S90
IF(21)で送信元=3000::2が転送設定とする
S91
設定要求：S91
(送信元=3000::2を遮断)
S92
IF(21)に送信元=3000::2を遮断設定する

フロントページの続き

(56)参考文献 特開２００２－３１４５８８（ＪＰ，Ａ）
特開２００４－０８６５３２（ＪＰ，Ａ）
特開２００３－３４８１４９（ＪＰ，Ａ）
特開２００３－１９６１４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／００－６６