(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2004-221879
(P2004-221879A)
(43)公開日　平成16年8月5日(2004.8.5)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/66	H04L 12/66	B	5K030
H04L 12/46	H04L 12/46	E	5K033
H04L 12/56	H04L 12/56	100Z	

審査請求 未請求　請求項の数 27　ＯＬ　（全 23 頁）

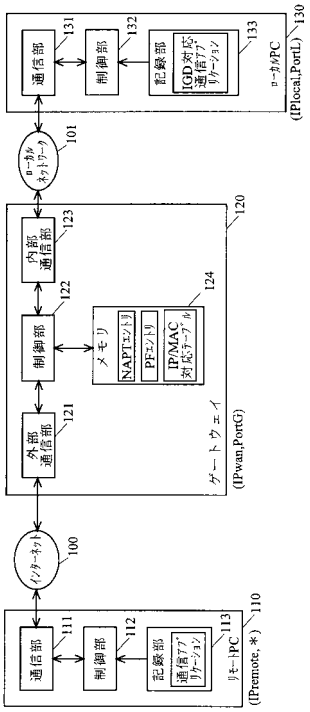
(21)出願番号　特願2003-6015(P2003-6015)
(22)出願日　平成15年1月14日(2003.1.14)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100098291
弁理士　小笠原　史朗
(72)発明者　濱本　望絵
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　古門　健
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

Ｆターム(参考)　5K030 GA15 HA08 HC01 HD03 HD09 JA11 KA05 LC15 MA06 MD09
5K033 AA08 CB09 DA06 DB12 DB18 EC03

(54)【発明の名称】通信方法、通信プログラムおよび中継装置

(57)【要約】
【課題】通信経路に関する情報の設定を、ユーザが手動で行うのではなく、ゲートウェイが通信を行う際に自動的に行うことができる通信方法を提供することを目的とする。
【解決手段】ゲートウェイ１２０は、インターネット１００とローカルネットワーク１０１との境界に配置されている。ローカルＰＣ１３０は、リモートＰＣ１１０とパケット通信を行いたい場合、ゲートウェイ１２０にＮＡＰＴの設定を要求する。ゲートウェイ１２０は、当該ＮＡＰＴの設定要求があった場合、パケットの通過および破棄を定義したパケットフィルタ（ＰＦ）エントリを作成する。ゲートウェイ１２０は、ＰＦエントリに基づいて、ローカルＰＣへのパケットの通過および破棄を判断する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
複数のネットワークの境界に配置されている中継装置において、任意の第１のネットワークから任意の第２のネットワークへ向けて送信されたパケットの通過を制限するための方法であって、
前記第２のネットワーク内に存在する任意の通信端末から前記第１のネットワーク内に存在する通信端末との間のアクセスに関連する情報が前記中継装置に入力された場合、当該アクセスに関連する情報から把握される前記第１および第２のネットワーク間の通信経路を解釈し、少なくとも当該通信経路を確保し得るパケット通過条件情報を前記中継装置が作成するステップと、
前記第２のネットワーク内の通信端末からパケットが送られてきた場合、前記通過条件情報に基づいて、当該パケットの通過可否を前記中継装置が判断するステップと、
前記通過可否の判断に基づいて、前記第２のネットワーク内の通信端末からのパケットを前記中継装置が通過あるいは破棄するステップとを備える、通信方法。
【請求項２】
前記通過条件情報を前記中継装置が作成するステップでは、前記アクセスに関連する情報を入力した通信端末から通知されるパラメータに基づいて通信経路を解釈し、必要に応じて、前記第１のネットワーク内に存在する通信端末から情報を取得することによって、前記通過条件情報を作成することを特徴とする、請求項１に記載の通信方法。
【請求項３】
前記通過条件情報を前記中継装置が作成するステップでは、さらに、前記パラメータで指定されているポート番号宛への最初のパケットの送信元を、前記第２のネットワークと交信可能な通信端末として、前記通過条件情報を作成することを特徴とする、請求項２に記載の通信方法。
【請求項４】
前記通過条件情報を前記中継装置が作成するステップでは、さらに、前記パラメータで指定されているポート番号を参照して、前記第２のネットワーク内に存在する任意の通信端末が交信相手を限定しているか否かを判断し、その判断結果に基づいて、前記通過条件情報を作成することを特徴とする、請求項２に記載の通信方法。
【請求項５】
前記アクセスに関連する情報を入力した通信端末が、前記第２のネットワーク内に存在する自端末以外の通信端末について、アクセスに関連する情報を入力してきた場合、
前記通過条件情報を前記中継装置が作成するステップでは、さらに、前記アクセスに関連する情報を入力した通信端末が、自端末以外の通信端末の通信経路を指定できる権利を有しているか否かを判断して、当該権利を有している場合のみ、指定された前記自端末以外の通信端末に関する通過条件情報を作成することを特徴とする、請求項２に記載の通信方法。
【請求項６】
前記通過条件情報を前記中継装置が作成するステップでは、さらに、前記アクセスに関連する情報を入力した通信端末が、自端末についての通信経路を指定してきた場合のみ、通過条件情報を作成することを特徴とする、請求項２に記載の通信方法。
【請求項７】
さらに、通信経路が確保されている前記第２のネットワーク内の通信端末が通信不能であるか否かを前記中継装置が判断するステップと、
当該通信端末が通信不能であると判断された場合、当該通信端末に関する通過条件情報を前記中継装置が削除するステップとを備える、請求項１に記載の通信方法。
【請求項８】
さらに、一定時間が経過したら前記通信条件情報を前記中継装置が削除するステップを備える、請求項１に記載の通信方法。
【請求項９】

さらに、通信経路が確保されている前記第２のネットワーク内の通信端末が再起動したか否かを前記中継装置が判断するステップと、
当該通信端末が再起動したと判断された場合、当該通信端末に関する通過条件情報を削除すべきか否かを前記中継装置が判断するステップと、
削除すべきと判断された場合、当該通過条件情報を前記中継装置が削除するステップとを備える、請求項１に記載の通信方法。
【請求項１０】
さらに、通信経路が確保されている前記第２のネットワーク内の通信端末の運用状態を監視するステップと、
運用状態の監視結果に応じて、当該通信端末に関する通過条件情報を削除するステップとを備える、請求項１に記載の通信方法。
【請求項１１】
前記運用状態を監視するステップでは、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（ＰａｃｋｅｔＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、前記通信経路が確保されている前記第２のネットワーク内の通信端末の運用状態を監視することを特徴とする、請求項１０に記載に通信方法。
【請求項１２】
さらに、前記アクセスに関連する情報を入力した通信端末の運用状態を監視するステップと、
運用状態の監視結果に応じて、通信経路が確保されている前記第２のネットワーク内の通信端末に関する通過条件情報を削除するステップとを備える、請求項１に記載の通信方法。
【請求項１３】
前記運用状態を監視するステップでは、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（ＰａｃｋｅｔＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、前記アクセスに関連する情報を入力した通信端末の運用状態を監視することを特徴とする、請求項１２に記載に通信方法。
【請求項１４】
請求項１～１３のいずれかに記載の通信方法をコンピュータ装置で実行するための通信プログラム。
【請求項１５】
複数のネットワークの境界に配置されており、任意の第１のネットワークから任意の第２のネットワークへ向けて送信されたパケットの通過を制限しながらパケットを中継する中継装置であって、
前記第２のネットワーク内に存在する任意の通信端末から前記第１のネットワーク内に存在する通信端末との間のアクセスに関連する情報が入力された場合、当該アクセスに関連する情報から把握される前記第１および第２のネットワーク間の通信経路を解釈し、少なくとも当該通信経路を確保し得るパケット通過条件情報を作成する通過条件情報作成手段と、
前記第２のネットワーク内の通信端末からパケットが送られてきた場合、前記通過条件情報作成手段が作成した前記通過条件情報に基づいて、当該パケットの通過可否を判断する通過可否判断手段と、
前記通過可否判断手段の判断に基づいて、前記第２のネットワーク内の通信端末からのパケットを通過あるいは破棄する通過制御手段とを備える、中継装置。
【請求項１６】
前記通過条件情報作成手段は、前記アクセスに関連する情報を入力した通信端末から通知されるパラメータに基づいて通信経路を解釈し、必要に応じて、前記第１のネットワーク

内に存在する通信端末から情報を取得することによって、前記通過条件情報を作成することを特徴とする、請求項１５に記載の中継装置。
【請求項１７】
前記通過条件情報作成手段は、さらに、前記パラメータで指定されているポート番号宛への最初のパケットの送信元を、前記第２のネットワークと交信可能な通信端末として、前記通過条件情報を作成することを特徴とする、請求項１６に記載の中継装置。
【請求項１８】
前記通過条件情報作成手段は、さらに、前記パラメータで指定されているポート番号を参照して、前記第２のネットワーク内に存在する任意の通信端末が交信相手を限定しているか否かを判断し、その判断結果に基づいて、前記通過条件情報を作成することを特徴とする、請求項１６に記載の中継装置。
【請求項１９】
前記アクセスに関連する情報を入力した通信端末が、前記第２のネットワーク内に存在する自端末以外の通信端末について、アクセスに関連する情報を入力してきた場合、
前記通過条件情報作成手段は、さらに、前記アクセスに関連する情報を入力した通信端末が、自端末以外の通信端末の通信経路を指定できる権利を有しているか否かを判断して、当該権利を有している場合のみ、指定された前記自端末以外の通信端末に関する通過条件情報を作成することを特徴とする、請求項１６に記載の中継装置。
【請求項２０】
前記通過条件情報作成手段は、さらに、前記アクセスに関連する情報を入力した通信端末が、自端末についての通信経路を指定してきた場合のみ、通過条件情報を作成することを特徴とする、請求項１６に記載の中継装置。
【請求項２１】
さらに、通信経路が確保されている前記第２のネットワーク内の通信端末が通信不能であるか否かを前記中継装置が判断する通信不能判断手段と、
前記通信不能判断手段によって当該通信端末が通信不能であると判断された場合、当該通信端末に関する通過条件情報を削除する通過条件情報削除手段とを備える、請求項１５に記載の中継装置。
【請求項２２】
さらに、一定時間が経過したら前記通信条件情報を削除する通過条件情報削除手段を備える、請求項１５に記載の中継装置。
【請求項２３】
さらに、通信経路が確保されている前記第２のネットワーク内の通信端末が再起動したか否かを前記中継装置が判断する再起動判断手段と、
前記再起動判断手段によって当該通信端末が再起動したと判断された場合、当該通信端末に関する通過条件情報を削除すべきか否かを判断する削除判断手段と、
前記削除判断手段によって削除すべきと判断された場合、当該通過条件情報を削除する通過条件情報削除手段とを備える、請求項１５に記載の中継装置。
【請求項２４】
さらに、通信経路が確保されている前記第２のネットワーク内の通信端末の運用状態を監視する運用状態監視手段と、
前記運用状態監視手段の監視結果に応じて、当該通信端末に関する通過条件情報を削除する通過条件情報削除手段とを備える、請求項１５に記載の中継装置。
【請求項２５】
前記運用状態監視手段は、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（Ｐａｃｋｅｔ ＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、前記通信経路が確保されている前記第２のネットワーク内の通信端末の運用状態を監視することを特徴とする、請求項２４に記載に中継装置。
【請求項２６】

さらに、前記アクセスに関連する情報を入力した通信端末の運用状態を監視する運用状態監視手段と、
前記運用状態監視手段の監視結果に応じて、通信経路が確保されている前記第２のネットワーク内の通信端末に関する通過条件情報を削除する通過条件情報削除手段とを備える、請求項１５に記載の中継装置。
【請求項２７】
前記運用状態監視手段は、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（Ｐａｃｋｅｔ ＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、前記アクセスに関連する情報を入力した通信端末の運用状態を監視することを特徴とする、請求項２６に記載に中継装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、異なるネットワーク環境下に存在する端末間における通信方法に関し、より特定的には、ファイアフォールを介在させてアクセスを制限するための通信方法に関する。
【０００２】
【従来の技術】
現在、ＣＡＴＶ（Ｃａｂｌｅ Ｔｅｌｅｖｉｓｉｏｎ）やＡＤＳＬ（Ａｓｙｍｍｅｔｒｉｃ Ｄｉｇｉｔａｌ Ｓｕｂｓｃｒｉｂｅｒ Ｌｉｎｅ）、ＦＴＴＨ（Ｆｉｂｅｒ Ｔｏ Ｔｈｅ Ｈｏｍｅ）などの急速な普及により、端末からインターネットへの接続は、常時接続が当たり前になりつつある。常時接続可能なネットワーク環境では、外部からの不正アクセスや通信データの盗聴等を防止し、セキュリティを確保するために、ファイアウォールを設置することが必要不可欠となる。
【０００３】
ファイアウォールは、一般的には、社内ネットワークなどのＬＡＮ（Ｌｏｃａｌ Ａｒｅａ Ｎｅｔｗｏｒｋ）とインターネットなどのＷＡＮ（Ｗｉｄｅ Ａｒｅａ Ｎｅｔｗｏｒｋ）との接続点、すなわち、ネットワークの境界部分に設置される。ファイアウォールは、通過するネットワークトラフィックを監視して、ルールに基づいた正当な通信のみを行えるようにして、不正な通信を検知する。
【０００４】
ファイアウォールの種類には、ＩＰヘッダに含まれている情報を元に通信を制御するパケットフィルタリング、アプリケーション層で通信を中継するアプリケーションゲートウェイ、各層からの情報を元にセッション単位でフィルタリングを行うステートフルインスペクション、ＴＣＰによって実現されるアプリケーション間の通信路（バーチャルサーキット）で中継するタイプのサーキットレベルゲートウェイなどがある。実際のシステムでは、これらを柔軟に組み合わせることによって、安全性の高いファイアウォールシステムを構築している。
【０００５】
しかし、内部ネットワーク上の正当なユーザであっても、外部ネットワークから内部ネットワークのサーバへの通信経路が分からない場合、ファイアウォールが介在することによって、外部ネットワークから内部ネットワークへの接続を確保することができず、内部ネットワークのサーバにアクセスすることができない場合がある。
【０００６】
このような状況を解決するため、ファイアウォールの設置された内部ネットワークのサーバへ、外部ネットワーク上のクライアントからファイアウォールを越えてアクセスすることを可能とするシステムが、特許文献１に提案されている。図８は、このような従来のシステムの構成を示す図である。
【０００７】
図８に示すシステムにおいて、ディレクトリサービスサーバ９０１は、インターネット９

００の外部からアクセスしてきたクライアント９０２のユーザが、ローカルネットワーク９０３上の正当なユーザであるか否かの認証を行う。正当なユーザであると認証された場合、ファイアウォール９０４は、ファイアウォール兼中継サーバプログラム９０５を実行し、ディレクトリデータベース９０６を参照して、当該ユーザに対して予め設定されている通信経路に関する情報を取得する。ファイアウォール９０４は、当該通信経路に関する情報に基づいて、クライアント９０２のユーザがサーバ９０７へアクセス可能か否かを判断し、アクセス可能である場合、クライアント９０２とサーバ９０７との通信を中継する。

【０００８】

【特許文献１】

特開平１０－１５４１１８号公報（第８頁、第１図）

【０００９】

【発明が解決しようとする課題】

しかし、上記従来のシステムでは、外部ネットワークから内部ネットワークにアクセスできるユーザの情報と、内部ネットワークにおける通信経路に関する情報とを、ディレクトリデータベース９０６に予め登録しておく必要がある。この登録は、ユーザが手動で行う必要があり、大変面倒である。

【００１０】

それゆえ、本発明の目的は、通信経路に関する情報の設定を、ユーザが手動で行うのではなく、ゲートウェイが通信を行う際に自動的に行うことができる通信方法を提供することである。

【００１１】

また、ファイアウォールの設定を自動で行おうとする場合、必要な情報が欠乏している場合があり、ファイアウォールの自動設定は、容易ではない。現在、ゲートウェイの設定を自動で行う方法がいくつか提案されているが、ファイアウォールの設定を自動で行う方法は、未だ存在しない。

【００１２】

ゲートウェイの設定を自動で行う方法として、例えば、ＵＰｎＰ（Ｕｎｉｖｅｒｓａｌ Ｐｌｕｇ ａｎｄ Ｐｌａｙ）フォーラムが規定したＩＧＤ（インターネットゲートウェイデバイス：Ｉｎｔｅｒｎｅｔ Ｇａｔｅｗａｙ Ｄｅｖｉｃｅ）の仕様（ＩｎｔｅｒｎｅｔＧａｔｅｗａｙＤｅｖｉｃｅ：１ Ｄｅｖｉｃｅ Ｔｅｍｐｌａｔｅ Ｖｅｒｓｉｏｎ １．０１）で示されているものがある。

【００１３】

当該仕様では、ローカルＰＣからＩＧＤに対して、ＮＡＰＴ（ＮｅｔｗｏｒｋＡｄｄｒｅｓｓ Ｐｏｒｔ Ｔｒａｎｓｌａｔｉｏｎ）の設定を自動で行う方法が規定されている。ＮＡＰＴは、ＮＡＴ（Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ）としてプライベートＩＰアドレスとグローバルＩＰアドレスとを対応付けると共に、通信ポート（以下、単にポートという）毎にプライベートＩＰアドレスとグローバルＩＰアドレスとを対応付ける。ＮＡＰＴが設定されることによって、外部ネットワーク（インターネット）上の通信端末と内部ネットワーク（ＬＡＮ）上の通信端末とのピア・ツー・ピア（Ｐ２Ｐ：ｐｅｅｒ－ｔｏ－ｐｅｅｒ）通信がポートを介して可能となる。

【００１４】

ところが、当該仕様では、ファイアウォールを設定するための方法については、規定されていない。したがって、ＵＰｎＰの仕様を用いて、ＩＧＤが、ファイアウォールの設定に必要な情報をローカルＰＣから全て収集することができないこととなる。

【００１５】

それゆえ、本発明のさらなる目的は、ＩＧＤの機能を持ったゲートウェイにおいて、ファイアウォールの通信経路に関する情報の生成に必要な情報を全て自動的に収集して、ファイアウォールの設定を自動的に行う通信方法を提供することである。

【００１６】

【課題を解決するための手段および発明の効果】
第１の発明は、複数のネットワークの境界に配置されている中継装置において、任意の第１のネットワークから任意の第２のネットワークへ向けて送信されたパケットの通過を制限するための方法であって、
第２のネットワーク内に存在する任意の通信端末から第１のネットワーク内に存在する通信端末との間のアクセスに関連する情報が中継装置に入力された場合、当該アクセスに関連する情報から把握される第１および第２のネットワーク間の通信経路を解釈し、少なくとも当該通信経路を確保し得るパケット通過条件情報を中継装置が作成するステップと、
第２のネットワーク内の通信端末からパケットが送られてきた場合、通過条件情報に基づいて、当該パケットの通過可否を中継装置が判断するステップと、
通過可否の判断に基づいて、第２のネットワーク内の通信端末からのパケットを中継装置が通過あるいは破棄するステップとを備える。
【００１７】
上記第１の発明によれば、中継装置に対して、他のネットワークとのアクセスに関連する情報が入力された場合、通信経路を解釈して、少なくとも当該通信経路を確保し得る通過条件情報が自動的に作成され、当該通過条件情報に基づいて、中継装置がパケットの通過を制限することとなる。したがって、ユーザが、中継装置に対して、わざわざ、パケットフィルタやファイアウォール等の設定しなくても、自動的に設定されることとなるので、ユーザ設定の煩わしさが解消されることとなる。
【００１８】
また、通信端末からアクセスに関連する情報が入力されるたびに、中継装置は、通過条件情報を作成することとなるので、所望の通信経路に応じて、通過条件情報が動的に設定されることとなる。
【００１９】
第２の発明は、第１の発明に従属する発明であって、通過条件情報を中継装置が作成するステップでは、アクセスに関連する情報を入力した通信端末から通知されるパラメータに基づいて通信経路を解釈し、必要に応じて、第１のネットワーク内に存在する通信端末から情報を取得することによって、通過条件情報を作成することを特徴とする。
【００２０】
上記第２の発明によれば、通過条件情報に必要な情報を、アクセスに関連する情報を入力した通信端末または第１のネットワーク内に存在する通信端末から取得することとなるので、ユーザの意図を通過条件情報に反映させることが可能となる。
【００２１】
第３の発明は、第２の発明に従属する発明であって、通過条件情報を中継装置が作成するステップでは、さらに、パラメータで指定されているポート番号宛への最初のパケットの送信元を、第２のネットワークと交信可能な通信端末として、通過条件情報を作成することを特徴とする。
【００２２】
通常、アクセスに関連する情報の入力があった直後に送られてくるパケットは、中継して欲しい通信端末から送られてきたものである場合が多い。
上記第３の発明によれば、最初に送られてくるパケットの送信元を交信可能な通信端末とするので、中継を要求しているユーザの意図を通過条件情報に反映させることが可能となる。
【００２３】
第４の発明は、第２の発明に従属する発明であって、通過条件情報を中継装置が作成するステップでは、さらに、パラメータで指定されているポート番号を参照して、第２のネットワーク内に存在する任意の通信端末が交信相手を限定しているか否かを判断し、その判断結果に基づいて、通過条件情報を作成することを特徴とする。
【００２４】
上記第４の発明によれば、ポート番号を参照して交信相手を限定するか否かが判断される

ので、中継装置は、通信端末側で意図されている交信相手を認識することが可能となる。特に、通信端末が不特定多数の通信端末との通信を希望しているのか、あるいは、ＩＰ電話のように特定の通信端末との通信を希望しているのかを認識するのに有効である。

【００２５】

第５の発明は、第２の発明に従属する発明であって、アクセスに関連する情報を入力した通信端末が、第２のネットワーク内に存在する自端末以外の通信端末について、アクセスに関連する情報を入力してきた場合、

通過条件情報を中継装置が作成するステップでは、さらに、アクセスに関連する情報を入力した通信端末が、自端末以外の通信端末の通信経路を指定できる権利を有しているか否かを判断して、当該権利を有している場合のみ、指定された自端末以外の通信端末に関する通過条件情報を作成することを特徴とする。

【００２６】

上記第５の発明によれば、一定の権利を有している通信端末に対しては、他の通信端末に関する通信経路を設定させることができ、それに伴って、中継装置は、通過条件情報を設定する。

【００２７】

第６の発明は、第２の発明に従属する発明であって、通過条件情報を中継装置が作成するステップでは、さらに、アクセスに関連する情報を入力した通信端末が、自端末についての通信経路を指定してきた場合のみ、通過条件情報を作成することを特徴とする。

【００２８】

上記第６の発明によれば、自端末の通信経路しか設定できず、結果、自端末の通信条件情報のみが設定されることとなるので、不正な通信条件情報の設定を防止することが可能となる。

【００２９】

第７の発明は、第１の発明に従属する発明であって、さらに、通信経路が確保されている第２のネットワーク内の通信端末が通信不能であるか否かを中継装置が判断するステップと、

当該通信端末が通信不能であると判断された場合、当該通信端末に関する通過条件情報を中継装置が削除するステップとを備える。

【００３０】

上記第７の発明によれば、通信端末が通信不能であれば、通過条件情報が削除されることとなるので、通過条件情報が不用意に長時間残り続けるのを防止することができ、不正アクセスの防止に貢献することが可能となる。

【００３１】

第８の発明は、第１の発明に従属する発明であって、さらに、一定時間が経過したら通信条件情報を中継装置が削除するステップを備える。

【００３２】

上記第８の発明によれば、一定時間が経過したら、強制的に通過条件情報が削除されることとなるので、通過条件情報が不用意に長時間残り続けるのを防止することができ、不正アクセスの防止に貢献することが可能となる。

【００３３】

第９の発明は、第１の発明に従属する発明であって、さらに、通信経路が確保されている第２のネットワーク内の通信端末が再起動したか否かを中継装置が判断するステップと、

当該通信端末が再起動したと判断された場合、当該通信端末に関する通過条件情報を削除すべきか否かを中継装置が判断するステップと、

削除すべきと判断された場合、当該通過条件情報を中継装置が削除するステップとを備える。

【００３４】

上記第９の発明によれば、通信端末が再起動するたびに、通過条件情報を削除するか否かを判断することとなるので、通過条件情報が不用意に長時間残り続けるのを防止すること

ができ、不正アクセスの防止に貢献することが可能となる。

【００３５】

第１０の発明は、第１の発明に従属する発明であって、さらに、通信経路が確保されている第２のネットワーク内の通信端末の運用状態を監視するステップと、

運用状態の監視結果に応じて、当該通信端末に関する通過条件情報を削除するステップとを備える。

【００３６】

上記第１０の発明によれば、通過条件情報が不用意に長時間残り続けるのを防止することができ、不正アクセスの防止に貢献することが可能となる。

【００３７】

第１１の発明は、第１０の発明に従属する発明であって、運用状態を監視するステップでは、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（Ｐａｃｋｅｔ ＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、通信経路が確保されている第２のネットワーク内の通信端末の運用状態を監視することを特徴とする。

【００３８】

上記第１１の発明によれば、一般的な規格で用いられているコマンドを用いて、運用状態を監視することが可能となるので、通過条件情報の削除機能を中継装置で容易に実装することが可能となる。

【００３９】

第１２の発明は、第１の発明に従属する発明であって、さらに、アクセスに関連する情報を入力した通信端末の運用状態を監視するステップと、

運用状態の監視結果に応じて、通信経路が確保されている第２のネットワーク内の通信端末に関する通過条件情報を削除するステップとを備える。

【００４０】

上記第１２の発明によれば、通過条件情報が不用意に長時間残り続けるのを防止することができ、不正アクセスの防止に貢献することが可能となる。

【００４１】

第１３の発明は、第１２の発明に従属する発明であって、運用状態を監視するステップでは、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（Ｐａｃｋｅｔ ＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、アクセスに関連する情報を入力した通信端末の運用状態を監視することを特徴とする。

【００４２】

上記第１３の発明によれば、一般的な規格で用いられているコマンドを用いて、運用状態を監視することが可能となるので、通過条件情報の削除機能を中継装置で容易に実現することが可能となる。

【００４３】

第１４の発明は、第１～１３の発明のいずれかの通信方法をコンピュータ装置で実行するための通信プログラムである。

【００４４】

上記第１４の発明の通信プログラムをゲートウェイやルータ等の汎用の中継装置にインストールすれば、本発明の通信方法を実現することが可能となる。

【００４５】

第１５の発明は、複数のネットワークの境界に配置されており、任意の第１のネットワークから任意の第２のネットワークへ向けて送信されたパケットの通過を制限しながらパケットを中継する中継装置であって、

第２のネットワーク内に存在する任意の通信端末から第１のネットワーク内に存在する通

信端末との間のアクセスに関連する情報が入力された場合、当該アクセスに関連する情報から把握される第１および第２のネットワーク間の通信経路を解釈し、少なくとも当該通信経路を確保し得るパケット通過条件情報を作成する通過条件情報作成手段と、
第２のネットワーク内の通信端末からパケットが送られてきた場合、通過条件情報作成手段が作成した通過条件情報に基づいて、当該パケットの通過可否を判断する通過可否判断手段と、
通過可否判断手段の判断に基づいて、第２のネットワーク内の通信端末からのパケットを通過あるいは破棄する通過制御手段とを備える。

【００４６】

第１６の発明は、第１５の発明に従属する発明であって、通過条件情報作成手段は、アクセスに関連する情報を入力した通信端末から通知されるパラメータに基づいて通信経路を解釈し、必要に応じて、第１のネットワーク内に存在する通信端末から情報を取得することによって、通過条件情報を作成することを特徴とする。

【００４７】

第１７の発明は、第１６の発明に従属する発明であって、通過条件情報作成手段は、さらに、パラメータで指定されているポート番号宛への最初のパケットの送信元を、第２のネットワークと交信可能な通信端末として、通過条件情報を作成することを特徴とする。

【００４８】

第１８の発明は、第１６の発明に従属する発明であって、通過条件情報作成手段は、さらに、パラメータで指定されているポート番号を参照して、第２のネットワーク内に存在する任意の通信端末が交信相手を限定しているか否かを判断し、その判断結果に基づいて、通過条件情報を作成することを特徴とする。

【００４９】

第１９の発明は、第１６の発明に従属する発明であって、アクセスに関連する情報を入力した通信端末が、第２のネットワーク内に存在する自端末以外の通信端末について、アクセスに関連する情報を入力してきた場合、
通過条件情報作成手段は、さらに、アクセスに関連する情報を入力した通信端末が、自端末以外の通信端末の通信経路を指定できる権利を有しているか否かを判断して、当該権利を有している場合のみ、指定された自端末以外の通信端末に関する通過条件情報を作成することを特徴とする。

【００５０】

第２０の発明は、第１６の発明に従属する発明であって、通過条件情報作成手段は、さらに、アクセスに関連する情報を入力した通信端末が、自端末についての通信経路を指定してきた場合のみ、通過条件情報を作成することを特徴とする。

【００５１】

第２１の発明は、第１５の発明に従属する発明であって、さらに、通信経路が確保されている第２のネットワーク内の通信端末が通信不能であるか否かを中継装置が判断する通信不能判断手段と、
通信不能判断手段によって当該通信端末が通信不能であると判断された場合、当該通信端末に関する通過条件情報を削除する通過条件情報削除手段とを備える。

【００５２】

第２２の発明は、第１５の発明に従属する発明であって、さらに、一定時間が経過したら通信条件情報を削除する通過条件情報削除手段を備える。

【００５３】

第２３の発明は、第１５の発明に従属する発明であって、さらに、通信経路が確保されている第２のネットワーク内の通信端末が再起動したか否かを中継装置が判断する再起動判断手段と、
再起動判断手段によって当該通信端末が再起動したと判断された場合、当該通信端末に関する通過条件情報を削除すべきか否かを判断する削除判断手段と、
削除判断手段によって削除すべきと判断された場合、当該通過条件情報を削除する通過条

件情報削除手段とを備える。

【００５４】

第２４の発明は、第１５の発明に従属する発明であって、さらに、通信経路が確保されている第２のネットワーク内の通信端末の運用状態を監視する運用状態監視手段と、

運用状態監視手段の監視結果に応じて、当該通信端末に関する通過条件情報を削除する通過条件情報削除手段とを備える。

【００５５】

第２５の発明は、第２４の発明に従属する発明であって、運用状態監視手段は、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（Ｐａｃｋｅｔ ＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、通信経路が確保されている第２のネットワーク内の通信端末の運用状態を監視することを特徴とする。

【００５６】

第２６の発明は、第１５の発明に従属する発明であって、さらに、アクセスに関連する情報を入力した通信端末の運用状態を監視する運用状態監視手段と、

運用状態監視手段の監視結果に応じて、通信経路が確保されている第２のネットワーク内の通信端末に関する通過条件情報を削除する通過条件情報削除手段とを備える。

【００５７】

第２７の発明は、第２６の発明に従属する発明であって、運用状態監視手段は、ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇ（Ｐａｃｋｅｔ ＩｎｔｅｒＮｅｔ Ｇｒｏｐｅｒ）もしくはＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）またはこれらの組み合わせによって、アクセスに関連する情報を入力した通信端末の運用状態を監視することを特徴とする。

【００５８】

第１５～第２７の発明によって得られる効果は、第１～第１３の発明によって得られる効果と同様である。

【００５９】

【発明の実施の形態】

図１は、本発明の実施形態に係るシステム全体の構成ならびにリモートＰＣ１１０、ゲートウェイ１２０およびローカルＰＣ１３０の構成を示す図である。図１において、当該システムは、インターネット１００に接続されたリモートＰＣ１１０と、インターネット１００およびローカルネットワーク１０１に接続されたゲートウェイ１２０と、ローカルネットワーク１０１に接続されたローカルＰＣ１３０とを備える。

【００６０】

なお、図１では、インターネット１００に接続されるリモートＰＣ１１０を一つだけ示したが、一つ以上であってもよく、さらに、ＰＣ以外のネットワーク通信端末が接続されていてもよい。また、ローカルネットワーク１０１に接続されるローカルＰＣ１３０を一つだけ示したが、一つ以上であってもよく、さらに、ＰＣ以外のネットワーク対応家電やネットワーク通信端末が接続されていてもよい。また、ここでは、二つのネットワーク（インターネットおよびローカルネットワーク）についての構成を示しているが、三つ以上のネットワーク（ローカルまたはグローバルを問わない）を含む構成であってもよい。

【００６１】

ゲートウェイ１２０には、グローバルＩＰアドレスとして、“ＩＰｗａｎ”が割り当てられているとする。リモートＰＣ１１０には、グローバルＩＰアドレスとして、“ＩＰｒｉｍｏｔｅ”が割り当てられているとする。以下、リモートＰＣ１１０のＩＰアドレスと言った場合、グローバルＩＰアドレスのことを言うものとする。ローカルＰＣ１３０には、プライベートＩＰアドレスとして、“ＩＰｌｏｃａｌ”が割り当てられているとする。

【００６２】

ゲートウェイ１２０は、インターネット１００とローカルネットワーク１０１との境界に

配置されている中継装置である。ローカルＰＣ１３０およびリモートＰＣ１１０は、ゲートウェイ１２０を介して、相互に通信する。

【００６３】

当該システムは、ゲートウェイ１２０に設定されているＮＡＰＴをローカルＰＣ１３０から遠隔制御するためのインターフェイスとして、ＵＰｎＰにおけるＩＧＤを用いる。

【００６４】

ゲートウェイ１２０は、外部通信部１２１と、制御部１２２と、内部通信部１２３と、メモリ１２４とを含む。メモリ１２４には、ＮＡＰＴエントリデータ（以下、単に、ＮＡＰＴエントリという）と、ＰＦ（Ｐａｃｋｅｔ　Ｆｉｌｔｅｒ）エントリデータ（以下、単に、ＰＦエントリという）と、ＩＰ／ＭＡＣ対応テーブルとが格納されている。

【００６５】

ＮＡＰＴエントリは、ＮＡＴとしてプライベートＩＰアドレスとグローバルＩＰアドレスとを対応付けるテーブルであると共に、ポート毎にプライベートＩＰアドレスとグローバルＩＰアドレスとを対応付けるテーブルである。ＮＡＰＴが設定されることによって、リモートＰＣ１１０とローカルＰＣ１３０とのピア・ツー・ピア通信がポートを介して可能となる。

【００６６】

ＰＦエントリは、インターネット１００上の通信端末から送られてくるパケットをローカルネットワーク１０１に通過させてよいか否かの通過条件情報を定めるテーブルであり、具体的には、ローカルネットワーク１０１上の通信端末宛に通過させてよいパケットの送信元グローバルＩＰアドレスを設定している。

【００６７】

ＩＰ／ＭＡＣ対応テーブルは、ローカルネットワーク１０１上の通信端末についてのプライベートＩＰアドレスとＭＡＣアドレスとを対応付けるテーブルである。

【００６８】

外部通信部１２１は、インターネット１００を介して、制御部１２２とリモートＰＣ１１０とが通信するための通信装置である。内部通信部１２３は、ローカルネットワーク１０１を介して、制御部１２２とローカルＰＣ１３０とが通信するための通信装置である。

【００６９】

制御部１２２は、ローカルネットワーク１０１に接続されている通信端末（ローカルＰＣ１３０やその他の通信端末等）の起動時に、ＩＰ／ＭＡＣ対応テーブルを作成し、メモリ１２４に格納する。

【００７０】

制御部１２２は、ＵＰｎＰにおけるＩＧＤ機能を有し、ローカルＰＣ１３０との間でＩＧＤ仕様による通信を行い、ローカルＰＣ１３０からの要求に応じてＮＡＰＴエントリを作成し、メモリ１２４に格納する。制御部１２２は、ＮＡＰＴエントリを参照することによって、ポートが指定されているローカルＰＣ１３０のグローバルＩＰアドレスをポートが指定されているプライベートＩＰアドレスに変換する。

【００７１】

制御部１２２は、ローカルＰＣ１３０からＮＡＰＴエントリの要求、すなわち、インターネット１００との間の通信経路に関する情報が入力された場合、ＰＦエントリを作成し、メモリ１２４に格納する。制御部１２２は、作成したＰＦエントリに基づいて、リモートＰＣ１１０からのパケットを通過するか否かを判断し、リモートＰＣ１１０とローカルＰＣ１３０との通信を実現する。

【００７２】

制御部１２２は、上記機能を有するプログラムがマスクされているＬＳＩ等である。なお、制御部１２２は、上記機能を有するプログラムを記録装置（図示せず）から読み込んで実行するような汎用のＣＰＵ（図示せず）であってもよい。上記機能については、後述の動作説明でより明らかとなる。

【００７３】

リモートＰＣ１１０は、通信部１１１と、制御部１１２と、記録部１１３とを含む。記録部１１３には、ＴＣＰ／ＩＰをプロトコルとする通信アプリケーションが格納されている。制御部１１２は、記録部１１３に格納されている通信アプリケーションを実行することによって、リモートＰＣ１１０の動作を制御する。

【００７４】

ローカルＰＣ１３０は、通信部１３１と、制御部１３２と、記録部１３３とを含む。記録部１３３には、ＩＧＤ仕様によってゲートウェイ１２０と通信するためのアプリケーション（以下、ＩＧＤ対応通信アプリケーションという）が格納されている。制御部１３２は、記録部１３３に格納されているＩＧＤ対応通信アプリケーションを実行することによって、ローカルＰＣ１３０の動作を制御する。

【００７５】

図２は、本実施形態に係るシステムにおいて、ローカルＰＣ１３０とリモートＰＣ１１０との間で通信を行う場合のシステム全体の動作を示す図である。以下、図２を参照しながら、システム全体の動作について説明する。

【００７６】

まず、初期設定として、ゲートウェイ１２０の制御部１２２は、ローカルＰＣ１３０またはゲートウェイ１２０に接続されているその他の機器が起動し、これらがゲートウェイ１２０に対してＤＨＣＰ（Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）によるプライベートＩＰアドレスの割当てを要求してきた際に、これらの機器に対してプライベートＩＰアドレスを割り当て、当該機器のＭＡＣアドレスを取得して、ＩＰ／ＭＡＣ対応テーブルを作成し、メモリ１２４に格納する（ステップＳ２００）。

【００７７】

ＩＧＤ対応通信アプリケーションを実行中のローカルＰＣ１３０は、インターネット１００上の通信端末と通信がしたい場合、インターネット１００とのアクセスに必要な通信経路に関連する情報として、“ゲートウェイの外向けポート番号”、“ローカルＰＣ１３０のプライベートＩＰアドレス”、“ローカルＰＣ１３０のポート番号”、“リモートＰＣのＩＰアドレス”、“通信プロトコル”、および“ＮＡＰＴエントリの有効期限”の６つのパラメータをゲートウェイ１２０に送信し、ＮＡＰＴの設定を要求する（ステップＳ２０１）。

【００７８】

なお、リモートＰＣ１１０以外の通信端末と通信したい場合、ローカルＰＣ１３０は、当該通信端末のＩＰアドレスを指定する。なお、ローカルＰＣ１３０は、インターネット１００上の通信端末のＩＰアドレスが分からない場合がある。このような場合、ローカルＰＣ１３０は、インターネット１００上のサーバ（図示せず）から、インターネット１００上の通信端末のＩＰアドレスを取得する。または、ローカルＰＣ１３０は、ＩＰアドレスを直接取得せずに、当該サーバを経由してインターネット１００上の通信端末にパケットが届くような情報をパケットのデータ部分に格納して送信する。本実施形態では、ローカルＰＣ１３０のＩＰアドレスを直接指定する方法を用いてもよいし、サーバ経由でローカルＰＣ１３０にパケットを送信する方法を用いてもよい。

【００７９】

このようなパラメータの設定は、ＩＧＤ対応通信アプリケーションに依存する。ＩＧＤ対応通信アプリケーションは、ユーザの入力に応じてパラメータを設定してもよいし、自動的にパラメータを設定してもよい。本実施形態におけるゲートウェイ１２０は、ＩＧＤ対応通信アプリケーションが如何なる方法でＮＡＰＴの設定を要求したとしても、ファイアウォールを提供できる。

【００８０】

ゲートウェイ１２０の制御部１２２は、ＮＡＰＴ設定要求を受け取ると、受け取ったパラメータに基づいて、インターネット１００とローカルネットワーク１０１との間の通信経路を解釈してＮＡＰＴエントリを作成し、メモリ１２４に格納する（ステップＳ２０２）

。
【００８１】
次に、制御部１２２は、解釈した通信経路に基づいて、ＰＦエントリを作成し、メモリ１２４に格納する（ステップＳ２０３）。具体的には、制御部１２２は、“リモートＰＣのＩＰアドレス”と、“ゲートウェイの外向けポート番号”、“ローカルＰＣ１３０のプライベートＩＰアドレス”、“ローカルＰＣ１３０のポート番号”、および“通信プロトコル”とを対応つけることによって、ＰＦエントリを作成する。
【００８２】
その後、通信アプリケーションを実行中のリモートＰＣ１１０は、通信データを含むパケットをローカルＰＣ１３０宛に送信する（ステップＳ２０４）。
【００８３】
ゲートウェイ１２０の制御部１２２は、リモートＰＣ１１０から送信されてくるパケットを受信し、当該パケットのヘッダを参照し、必要に応じて、ＰＦエントリを再設定する（ステップＳ２０５）。ＰＦエントリの設定または再設定によって、パラメータに基づいて解釈された通信経路を少なくとも確保するリモートＰＣ１１０とローカルＰＣ１３０との間の通信経路がＰＦエントリに設定されることとなる。
【００８４】
次に、制御部１２２は、ＮＡＰＴエントリを参照して、ローカルＰＣ１３０のプライベートＩＰアドレスを取得し、ＰＦエントリを参照して、当該パケットをローカルＰＣ１３０宛に通過させて良いか否かを判断し、通過させて良い場合、ローカルＰＣ１３０に対して、当該パケットを送信する（ステップＳ２０６）。
【００８５】
次に、ローカルＰＣ１３０は、ゲートウェイ１２０から送られてくるパケットを受信する（ステップＳ２０７）。
【００８６】
その後、リモートＰＣ１１０は、ローカルＰＣ１３０宛のパケットを送信したり、あるいはローカルＰＣ１３０からのパケットを受信したりして（ステップＳ２０８）、処理を終了する。
【００８７】
ゲートウェイ１２０の制御部１２２は、リモートＰＣ１１０からのパケットを受信し、ＮＡＰＴエントリを参照して、当該パケットの宛先であるローカルＰＣ１３０のプライベートＩＰアドレスを取得し、ＰＦエントリを参照して、当該パケットをローカルＰＣ１３０宛に通過させて良いか否かを判断し、通過させて良い場合、当該パケットをローカルＰＣ１３０に送信する（ステップＳ２０９）。あるいは、ゲートウェイ１２０の制御部１２２は、ローカルＰＣ１３０からのパケットを受信してリモートＰＣ１１０に送信して（ステップＳ２０９）、処理を終了する。
【００８８】
ローカルＰＣ１３０は、ゲートウェイ１２０を介して送られてくるリモートＰＣ１１０からのパケットを受信したり、あるいはリモートＰＣ１１０宛のパケットをゲートウェイ１２０に送信したりして（ステップＳ２１０）、処理を終了する。ステップＳ２０８～Ｓ２１０の処理によって、ローカルＰＣ１３０とリモートＰＣ１１０とのピア・ツー・ピア通信が可能となる。
【００８９】
図３は、ＮＡＰＴエントリを設定するときのゲートウェイ１２０の動作を示すフローチャートである。図３に示すフローチャートは、図２におけるステップＳ２０２を詳細に示したものである。以下、図３を参照しながら、ＮＡＰＴエントリを作成するときのゲートウェイ１２０の動作について説明する。
【００９０】
まず、ゲートウェイ１２０の制御部１２２は、ローカルＰＣ１３０からＮＡＰＴの設定要求があるか否かを判断する（ステップＳ３０１）。ＮＡＰＴの設定要求がない場合、制御

部１２２は、ステップＳ３０１の動作に戻る。一方、ＮＡＰＴの設定要求がある場合、制御部１２２は、ステップＳ３０２の動作に進む。

【００９１】

ローカルＰＣ１３０は、ＮＡＰＴの設定要求を行う場合、パラメータ（たとえば、（ＰｏｒｔＧ，ＩＰｌｏｃａｌ，ＰｏｒｔＬ，＊，ＴＣＰ，３６００））をゲートウェイ１２０に送信する。ここで、“ＰｏｒｔＧ”は、ゲートウェイの外向けポート番号を示す。“ＩＰｌｏｃａｌ”は、ローカルＰＣのプライベートＩＰアドレスを示す。“ＰｏｒｔＬ”は、ローカルＰＣのポート番号を示す。“＊”は、リモートＰＣのＩＰアドレスとして任意のアドレスを指定することを意味する。最後から二つ目のパラメータ“ＴＣＰ”は、ローカルＰＣとリモートＰＣとが通信する際に使用するプロトコルである。最後のパラメータ“３６００”は、ＮＡＰＴエントリの有効期限が３６００秒であることを示す。

【００９２】

ステップＳ３０２において、制御部１２２は、ＮＡＰＴの設定を要求してきたローカルＰＣ１３０のプライベートＩＰアドレスおよびＭＡＣアドレスを、ＮＡＰＴ設定要求パケットのヘッダ部から取得する（ステップＳ３０２）。次に、制御部１２２は、初期設定時（ステップＳ２００参照）に作成したＩＰ／ＭＡＣ対応テーブルを参照し、ステップＳ３０２で取得したプライベートＩＰアドレスおよびＭＡＣアドレスがＩＰ／ＭＡＣ対応テーブルの内容と一致しているか否かを判断する（ステップＳ３０３）。

【００９３】

一致しない場合、制御部１２２は、ＮＡＰＴエントリの設定を許可しない旨をローカルＰＣ１３０に通知し（ステップＳ３０４）、処理を終了する。一方、一致する場合、制御部１２２は、ステップＳ３０５の動作に進む。

【００９４】

ステップＳ３０５において、制御部１２２は、ローカルＰＣ１３０から送られてくるパラメータを参照して、“ローカルＰＣのプライベートＩＰアドレス”を取得する（ステップＳ３０５）。

【００９５】

次に、制御部１２２は、ステップＳ３０２においてローカルＰＣ１３０から直接取得したプライベートＩＰアドレスと、パラメータから取得したローカルＰＣのＩＰアドレスとを比較し、これらが一致しているか否かを判断する（ステップＳ３０６）。これは、ローカルＰＣ１３０が、自機器以外の機器のＮＡＰＴエントリを要求していないことを確認するための処理である。

【００９６】

ＩＰアドレスが一致しない場合、制御部１２２は、ステップＳ３０４の動作に進み、不許可を通知して、処理を終了する。一方、ＩＰアドレスが一致する場合、制御部１２２は、ローカルＰＣ１３０から受け取ったパラメータに基づいて、ＮＡＰＴエントリを作成してメモリ１２４に格納し（ステップＳ３０７）、処理を終了する。

【００９７】

図４は、ＰＦエントリを設定するときのゲートウェイ１２０の動作を示すフローチャートである。図４は、図２におけるステップＳ２０３およびＳ２０５の動作を詳細に示したフローチャートである。以下、図４を参照しながら、ＰＦエントリを設定するときのゲートウェイ１２０の動作について説明する。

【００９８】

ゲートウェイ１２０の制御部１２２は、ＮＡＰＴエントリで用いたパラメータと同じパラメータを利用して、ＰＦエントリを作成し、メモリ１２４に格納する（ステップＳ４０１）。

【００９９】

たとえば、ローカルＰＣ１３０が、ＮＡＰＴ設定要求のためのパラメータとして、（ＰｏｒｔＧ，ＩＰｌｏｃａｌ，ＰｏｒｔＬ，＊，ＴＣＰ，３６００）をゲートウェイ１２０に送信したとする。ＩＧＤ対応通信アプリケーションの種類によっては、上記パラメータの

ように、リモートＰＣのＩＰアドレスを“＊”として任意のものであると指定する場合がある。リモートＰＣのＩＰアドレスが任意の場合、“ＰｏｒｔＧ”宛のパケットが全てローカルＰＣ１３０に送られることとなる。これでは、不都合が生じる場合がある。

【０１００】

そのため、制御部１２２は、ローカルＰＣ１３０から送られてきたパラメータに含まれるローカルＰＣのポート番号を参照して、ローカルＰＣ１３０がＩＰ電話のようにピア・ツー・ピアで通信をしようとしているのか、それとも多数のクライアントからの接続を待っているのか、どちらであるのかを判断する（ステップＳ４０２）。

【０１０１】

具体的には、制御部１２２は、ウェルノウンポート番号およびそのサービスの一覧のテーブルをメモリ１２４に格納しておき、当該テーブルを参照して、ステップＳ４０２の判断を行う。ローカルＰＣ１３０からのパラメータに含まれているポート番号が８０番のＨＴＴＰなどのように多数のクライアントが接続するサービスを示しているのであれば、制御部１２２は、ローカルＰＣ１３０が多数のクライアントからの接続を待っていると判断する。

【０１０２】

ステップＳ４０２において、多数のクライアントからの接続を待っていると判断した場合、制御部１２２は、ＰＦエントリの設定をそのままの状態にして、処理を終了する。

【０１０３】

一方、ピア・ツー・ピアで通信しようとしていると判断した場合、制御部１２２は、パラメータを参照して、リモートＰＣのＩＰアドレスが指定されているか否かを判断する（ステップＳ４０３）。リモートＰＣのＩＰアドレスが指定されている場合、ＰＦエントリには、既にリモートＰＣのＩＰアドレスが設定されていることとなるので、制御部１２２は、ＰＦエントリの設定をそのままの状態にして、処理を終了する。一方、リモートＰＣのＩＰアドレスが指定されていない場合、制御部１２２は、ステップＳ４０４の動作に進む。

【０１０４】

上記一例で示したパラメータ“＊”のように、リモートＰＣのＩＰアドレスが指定されていない場合、アクセス可能なリモートＰＣを制限する必要がある。そのため、制御部１２２は、“ＰｏｒｔＧ”宛に最初に送信されたパケットのヘッダを参照し、送信元であるリモートＰＣのＩＰアドレス“ＩＰｒｅｍｏｔｅ”を取得する（ステップＳ４０４）。次に、制御部１２２は、取得したリモートＰＣのＩＰアドレスをＰＦエントリに登録することによって、ＰＦエントリを再設定し（ステップＳ４０５）、処理を終了する。

【０１０５】

たとえば、再設定後、制御部１２２は、“ＰｏｒｔＧ”宛のパケットのうち、ＩＰアドレスが“ＩＰｒｅｍｏｔｅ”のリモートＰＣ１１０からのパケットのみを通過し、それ以外の外部通信端末からのパケットを破棄する。

【０１０６】

このように、本実施形態に係るシステムでは、ローカルＰＣ１３０がＩＧＤ対応通信アプリケーションを実行しＮＡＰＴエントリの設定を要求した場合、すなわち、ローカルＰＣ１３０がローカルネットワーク１０１とインターネット１００との間のアクセスに関連する情報をゲートウェイ１２０に入力した場合、ゲートウェイ１２０は、要求されている通信経路を解釈して、少なくとも当該通信経路を確保し得る通信条件情報をＰＦエントリとして、自動的に作成する。ゲートウェイ１２０は、その後の通信において、ＰＦエントリを参照して外部端末からのパケットを通過するか否かを判断し、通過可能なパケットのみをローカルＰＣ１３０に送信する。したがって、ユーザが、ゲートウェイ１２０でファイアウォールに関する情報を設定しなくても、自動的にゲートウェイがファイアウォールに必要な設定を行うこととなる。

【０１０７】

また、ローカルＰＣ１３０からパケットのＮＡＰＴの設定要求がなされるたびに、ゲート

ウェイ１２０は、ＰＦエントリを作成することとなるので、ローカルＰＣ１３０の要求に応じて、ＰＦエントリを動的に設定することが可能となる。

【０１０８】

なお、本実施形態では、インターネット１００からローカルネットワーク１０１へのアクセス制限についてのみ説明したが、ゲートウェイ１２０は、二つのローカルネットワークの境界に配置されており、互いのローカルネットワーク間でのアクセス制限を行うようにＰＦエントリを設定するようにしてもよい。

【０１０９】

なお、本実施形態では、パケットの中継装置として、ゲートウェイを用いることとしたが、ルータ等の中継装置であってもよい。

【０１１０】

なお、本実施形態では、ゲートウェイ１２０のポートに最初に送られてきたパケットの送信元ＩＰアドレスに基づいて、ＰＦエントリを作成することとした。しかし、最初に送られてくるパケットの判断基準としては、ゲートウェイ１２０のポートに限られるものではない。ゲートウェイ１２０は、ローカルＰＣ１３０との対応が分かる情報、たとえば、ローカルＰＣ１３０宛の最初のパケットの送信元ＩＰアドレスに基づいて、ＰＦエントリを作成してもよい。

【０１１１】

なお、本実施形態では、通信形態を判断する場合（ステップＳ４０２参照）、ウェルノウンポート番号とそのサービス一覧とのテーブルを制御部１２２のメモリ１２４に格納し、当該テーブルを参照して判断することとしたが、ウェルノウンポートに限定されるものではなく、独自に規定したものを制御部１２２のテーブルに登録して判断するようにしてもよい。

【０１１２】

なお、上記実施形態では、ＵＰｎＰにおけるＩＧＤを用いて、ゲートウェイ１２０とローカルＰＣ１３０との間で通信を行うこととしているが、ＩＧＤに限られるものではなく、遠隔からゲートウェイのＮＡＰＴを操作できる仕様を用いた通信であれば、他の仕様であってもよい。

【０１１３】

なお、上記実施形態では、ローカルＰＣ１３０のＩＧＤ対応通信アプリケーションがＮＡＰＴエントリの設定要求を行う場合、ゲートウェイ１２０は、当該ローカルＰＣ１３０以外の機器についてのＮＡＰＴエントリの設定要求を拒否することとした（図３ステップＳ３０６参照）。しかし、これは本発明の一実施形態であり、これに限られるものではない。制御部１２２は、ローカルＰＣ１３０のアドレス情報と要求したＮＡＰＴエントリの情報とを用いて、より詳細なＮＡＰＴ設定についての制限を加えてもよいことは、言うまでもない。

【０１１４】

たとえば、制御部１２２は、ＮＡＰＴ設定を要求してきたローカルＰＣをアドレス情報によって識別し、他機器のＮＡＰＴ設定を行う権利を有しているローカルＰＣであるか否かを判断して、当該権利を有している場合、ＮＡＰＴ設定を行うようにしてもよい。

【０１１５】

また、制御部１２２は、ＮＡＰＴ設定パラメータ（ゲートウェイの外向けポート番号，ローカルＰＣのプライベートＩＰアドレス，ローカルＰＣのポート番号，リモートＰＣのＩＰアドレス，通信プロトコル，ＮＡＰＴエントリの有効期限）の各要素、あるいはその組み合わせと、要求送信元のローカルＰＣのアドレス情報とによって、ローカルＰＣに他機器のＮＡＰＴ設定の権利があるか否かを判断して、他機器のＮＡＰＴを設定してもよい。

【０１１６】

（ＮＡＰＴエントリおよびＰＦエントリの削除について）

ローカルＰＣ１３０がＮＡＰＴエントリの設定要求の際に送信するパラメータにおいて、ＮＡＰＴエントリの有効期限が“０”であると指定されている場合、作成されたＮＡＰＴ

エントリおよびＰＦエントリが、ゲートウェイ１２０のメモリ１２４上に残り続ける場合がある。

【０１１７】

図５は、ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止するために行われる削除処理の一例を実行したときのゲートウェイ１２０の動作を示すフローチャートである。以下、図５を参照しながら、ＮＡＰＴエントリが残り続けることを防止するための削除処理について説明する。以下で説明する削除処理は、ゲートウェイ１２０の制御部１２２において、他の処理と並行して行われている。

【０１１８】

まず、制御部１２２は、ＮＡＰＴエントリおよびＰＦエントリの設定を行ったか否かを、ＮＡＰＴエントリに登録されているリモートＰＣ毎に判断する（ステップＳ５０１）。ＮＡＰＴエントリおよびＰＦエントリの設定を行っていない場合、制御部１２２は、ステップＳ５０１の動作に戻る。一方、ＮＡＰＴエントリおよびＰＦエントリの設定を行っている場合、制御部１２２は、現在の時刻を取得する（ステップＳ５０２）。

【０１１９】

次に、制御部１２２は、一定時間が経過しているか否かを判断する（ステップＳ５０３）。経過していない場合、制御部１２２は、ステップＳ５０３の動作に戻る。

【０１２０】

一方、経過している場合、制御部１２２は、ＮＡＰＴエントリを参照して、ローカルＰＣ１３０のプライベートＩＰアドレスを取得し、当該ローカルＰＣ１３０に対して、たとえばｐｉｎｇ（Ｐａｃｋｅｔ　ＩｎｔｅｒＮｅｔ　Ｇｒｏｐｅｒ）コマンドなどを用いて、生存確認を問い合わせる（ステップＳ５０４）。

【０１２１】

次に、制御部１２２は、生存確認の問い合わせに対して、ローカルＰＣ１３０からの応答があるか否かを判断する（ステップＳ５０５）。応答がある場合、制御部１２２は、経過時刻をリセットして、ステップＳ５０２の動作に戻る。一方、応答がない場合、制御部１２２は、ローカルＰＣ１３０は通信不能な状態であると判断して、当該ローカルＰＣ１３０に対応するＮＡＰＴエントリおよびＰＦエントリを削除し（ステップＳ５０６）、処理を終了する。

【０１２２】

このように、ＮＡＰＴエントリおよびＰＦエントリを必要に応じて、定期的に削除することによって、長期に渡って、ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止することが可能となる。結果、ＮＡＰＴエントリおよびＰＦエントリが残り続けることよる弊害（たとえば、外部からの不正アクセスによって不正侵入）を防止することが可能となる。

【０１２３】

なお、上記では、ＮＡＰＴエントリおよびＰＦエントリの両方を削除することしたが、どちらか一方、たとえば、ＰＦエントリのみを削除するようにしてもよい。

【０１２４】

なお、ローカルＰＣが運用状態を監視する方法として、ｐｉｎｇコマンドによる応答の有無を用いることとしたが、ｐｉｎｇコマンドでなくても、なんらかの応答が返ってくる方法を用いるのであれば、何でもよい。たとえば、ＮＡＰＴエントリの設定を要求したローカルＰＣが通信可能な状態であるかをＡＲＰ（Ａｄｄｒｅｓｓ　Ｒｅｓｏｌｕｔｉｏｎ　Ｐｒｏｔｏｃｏｌ）、ｐｉｎｇもしくはＤＨＣＰまたはこれらの組み合わせにより運用状態を監視し、通信不能と判断した場合に、そのローカルＰＣに対応するＮＡＰＴエントリおよびＰＦエントリを削除するようにしてもよい。

【０１２５】

なお、上記では、ステップＳ５０４において、ＮＡＰＴエントリの設定を要求したローカルＰＣ１３０の運用状態を監視することとしたが、ローカルＰＣ１３０が他の通信端末のＮＡＰＴエントリの設定を要求した場合、当該他の通信端末の運用状態を監視するように

してもよい。

【０１２６】

図６は、ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止するために行われる削除処理の他の例を実行したときのゲートウェイ１２０の動作を示すフローチャートである。図６に示すように、制御部１２２は、ＮＡＰＴエントリおよびＰＦエントリを設定したか否かを判断した後（ステップＳ６０１）、現在の時刻を取得して（ステップＳ６０２）、一定時間（例えば２４時間）が経過しているか否かを判断し（ステップＳ６０３）、経過していればＮＡＰＴエントリおよびＰＦエントリを削除して（ステップＳ６０４）、処理を終了する。

【０１２７】

これにより、一定時間経過後に、自動的にＮＡＰＴエントリおよびＰＦエントリが削除されることとなる。

【０１２８】

なお、ここでは一定時間を２４時間としているが、この時間はユーザのニーズに合わせて自由に設定できるようにしてよい。

【０１２９】

図７は、ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止するために行われる削除処理の他の例を実行したときのゲートウェイ１２０の動作を示すフローチャートである。まず、制御部１２２は、ＮＡＰＴエントリおよびＰＦエントリを設定したか否かを判断する（ステップＳ７０１）。次に、制御部１２２は、ローカルＰＣ１３０のＭＡＣアドレスを取得する（ステップＳ７０２）。次に、制御部１２２は、取得したＭＡＣアドレスを設定したＮＡＰＴエントリと関連付けておくテーブルをメモリ１２４に格納する（ステップＳ７０３）。

【０１３０】

次に、制御部１２２は、ＤＨＣＰ再リクエスト要求を検出するか否かを判断する（ステップＳ７０４）。これは、ローカルＰＣ１３０が、再起動時に、ゲートウェイ１２０に対して、ＤＨＣＰ再リクエストを要求するという機能を利用している。

【０１３１】

ＤＨＣＰ再リクエスト要求を検出しない場合、制御部１２２は、ステップＳ７０４の動作に戻る。一方、ＤＨＣＰ再リクエスト要求を検出した場合、制御部１２２は、リクエストしてきたローカルＰＣのＭＡＣアドレスを取得する（ステップＳ７０５）。

【０１３２】

次に、制御部１２２は、取得したＭＡＣアドレスに対応するＮＡＰＴエントリおよびＰＦエントリが存在するか否かを判断する（ステップＳ７０６）。存在する場合、制御部１２２は、当該ＮＡＰＴエントリおよびＰＦエントリを削除して（ステップＳ７０７）、処理を終了する。一方、存在しない場合、制御部１２２は、そのまま処理を終了する。

【０１３３】

これにより、ローカルＰＣの起動時にＮＡＰＴエントリおよびＰＦエントリを削除するか否かを判断するので、長期間ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止することが可能となる。

【０１３４】

なお、上記ステップＳ７０６以降では、ＭＡＣアドレスと一致するＮＡＰＴエントリおよびＰＦエントリがある場合に、ＮＡＰＴエントリを削除することとしたが、別に、一致するエントリがない場合に、ＮＡＰＴエントリを削除するようにしてもよい。

【０１３５】

なお、上記では、ローカルＰＣの運用状態として、再起動の有無を判断することとしたが、別に、再起動以外の運用状態を判断するようにしてもよい。

【０１３６】

なお、上記では、ローカルＰＣが再起動したことを検出する方法として、ＤＨＣＰリクエストを用いることとしているが、ＤＨＣＰリクエストを検出する方法でなくても、ローカ

ルＰＣが再起動したことがわかる方法であれば、何でもよい。また、機器判別にＭＡＣアドレスを用いることとしているが、ＭＡＣアドレスでなくても、機器を一意に識別できるのであれば何でもよい。

【０１３７】

なお、上記では、ゲートウェイ１２０で自動的に作成されたＮＡＰＴエントリおよびＰＦエントリを削除の対象としたが、別に、ゲートウェイ１２０のユーザインターフェイスを利用してユーザが直接設定したＮＡＰＴエントリおよびＰＦエントリを削除の対象としてもよい。この場合も、ゲートウェイ１２０は、他の処理と並行して、図５～図７に示したような削除処理を行い、ユーザによって設定されたＮＡＰＴエントリおよびＰＦエントリを削除する。これにより、ＮＡＰＴエントリおよＰＦエントリが長時間残り続けることを防止することが可能となり、セキュリティーの向上につながる。当然、ＮＡＰＴエントリまたはＰＦエントリのどちらか一方を削除の対象としてもよいことは、言うまでもない。たとえば、ゲートウェイ１２０は、ユーザが直接設定したＮＡＰＴエントリに対して、一定期間（たとえば、１０日間）生存確認がとれないローカルＰＣに関するＮＡＰＴエントリおよびＰＦエントリを削除するようにしてもよい。

【０１３８】

なお、本実施形態では、設定されたＮＡＰＴエントリを削除する方法として、３種類の方法（図５～図７参照）を挙げたが、この３種類のうち、いずれか２種類または３種類を組み合わせてＮＡＰＴエントリを削除するとしてもよい。

【０１３９】

なお、ＮＡＰＴエントリおよびＰＦエントリの削除の条件としては、ＮＡＰＴエントリの有効期限を永久とするものに限られず、ある一定時間がＮＡＰＴエントリの有効期限とするものも削除の対象としてよい。

【図面の簡単な説明】

【図１】本発明の実施形態に係るシステム全体の構成ならびにリモートＰＣ１１０、ゲートウェイ１２０およびローカルＰＣ１３０の構成を示す図である。

【図２】本実施形態に係るシステムにおいて、ローカルＰＣ１３０とリモートＰＣ１１０との間で通信を行う場合のシステム全体の動作を示す図である。

【図３】ＮＡＰＴエントリを設定するときのゲートウェイ１２０の動作を示すフローチャートである。

【図４】ＰＦエントリを設定するときのゲートウェイ１２０の動作を示すフローチャートである。

【図５】ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止するために行われる削除処理の一例を実行したときのゲートウェイ１２０の動作を示すフローチャートである。

【図６】ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止するために行われる削除処理の他の例を実行したときのゲートウェイ１２０の動作を示すフローチャートである。

【図７】ＮＡＰＴエントリおよびＰＦエントリが残り続けることを防止するために行われる削除処理の他の例を実行したときのゲートウェイ１２０の動作を示すフローチャートである。

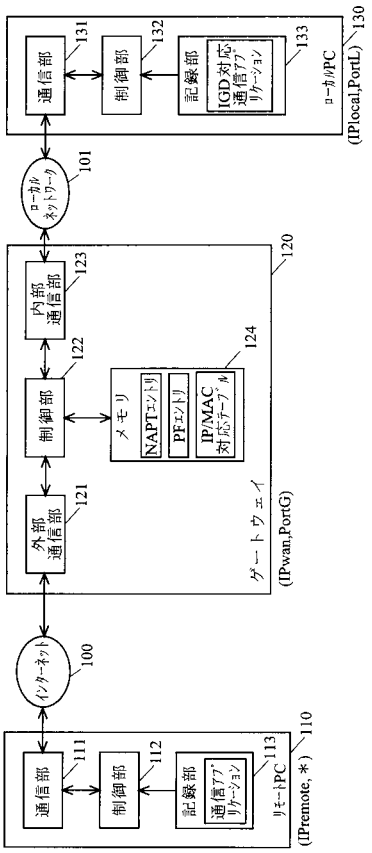
【図８】従来のシステムの構成を示す図である。

【符号の説明】

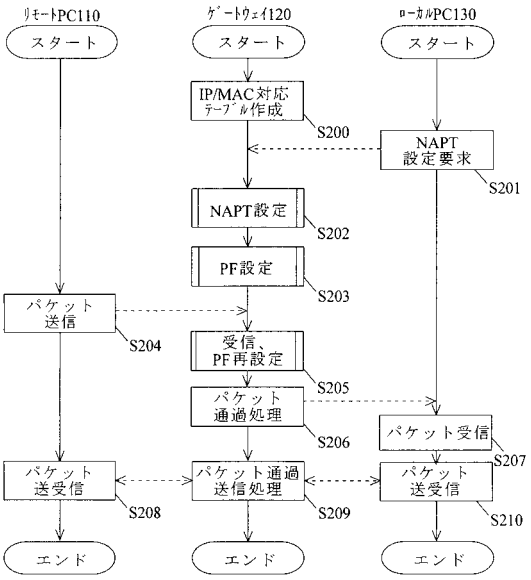
１００　インターネット
１０１　ローカルネットワーク
１１０　リモートＰＣ
１１１，１３１　通信部
１１２，１３２，１２２　制御部
１１３，１３３　記録部
１２０　ゲートウェイ

１２１　外部通信部
１２３　内部通信部
１２４　メモリ
１３０　ローカルＰＣ

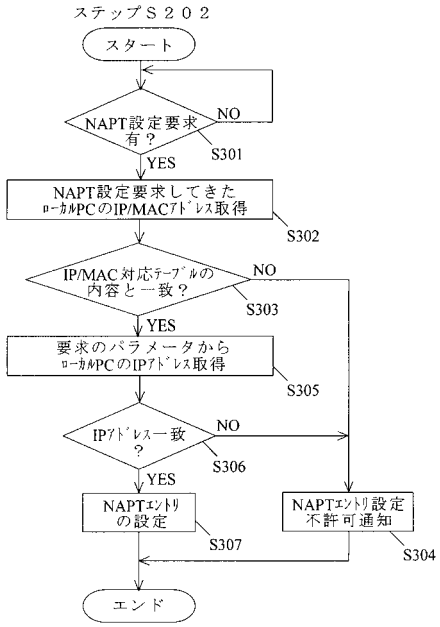
【図１】



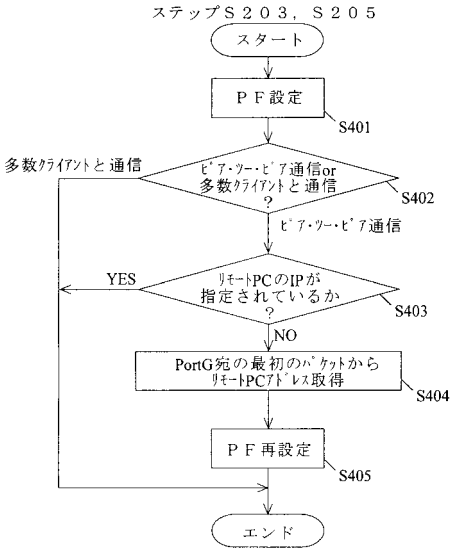
【図２】



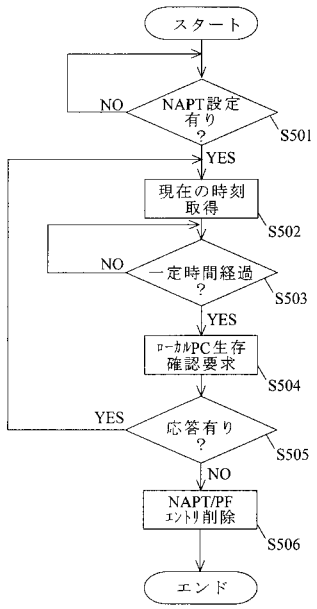
【図３】


ステップＳ２０２
スタート
NAPT設定要求有？
NO
S301
YES
NAPT設定要求してきたﾛｰｶﾙPCのIP/MACｱﾄﾞﾚｽ取得
S302
IP/MAC対応ﾃｰﾌﾞﾙの内容と一致？
NO
S303
YES
要求のパラメータからﾛｰｶﾙPCのIPｱﾄﾞﾚｽ取得
S305
IPｱﾄﾞﾚｽ一致？
NO
S306
YES
NAPTｴﾝﾄﾘの設定
S307
NAPTｴﾝﾄﾘ設定不許可通知
S304
エンド

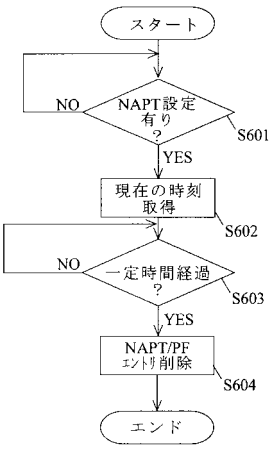
【図４】


ステップＳ２０３，Ｓ２０５
スタート
ＰＦ設定
S401
多数ｸﾗｲｱﾝﾄと通信
ﾋﾟｱ･ﾂｰ･ﾋﾟｱ通信or多数ｸﾗｲｱﾝﾄと通信？
S402
ﾋﾟｱ･ﾂｰ･ﾋﾟｱ通信
YES
ﾘﾓｰﾄPCのIPが指定されているか？
S403
NO
PortG宛の最初のﾊﾟｹｯﾄからﾘﾓｰﾄPCｱﾄﾞﾚｽ取得
S404
ＰＦ再設定
S405
エンド

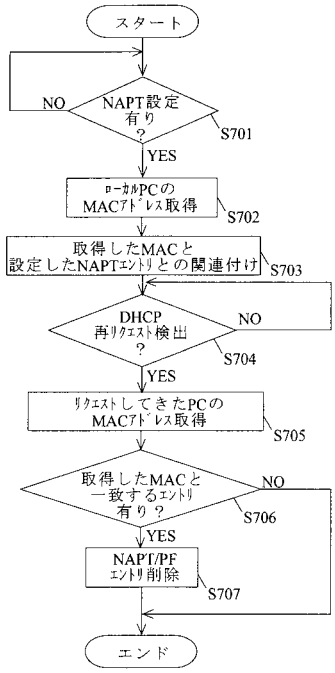
【図５】


スタート
NAPT設定有り？
NO
S501
YES
現在の時刻取得
S502
一定時間経過？
NO
S503
YES
ﾛｰｶﾙPC生存確認要求
S504
応答有り？
YES
S505
NO
NAPT/PFｴﾝﾄﾘ削除
S506
エンド

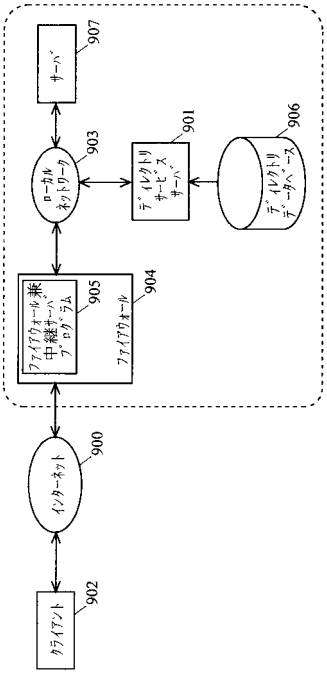
【図６】


スタート
NAPT設定有り？
NO
S601
YES
現在の時刻取得
S602
一定時間経過？
NO
S603
YES
NAPT/PFｴﾝﾄﾘ削除
S604
エンド

【図７】


スタート
NAPT設定有り？
NO
YES
S701
ローカルPCのMACアドレス取得
S702
取得したMACと設定したNAPTエントリとの関連付け
S703
DHCP再リクエスト検出？
NO
YES
S704
リクエストしてきたPCのMACアドレス取得
S705
取得したMACと一致するエントリ有り？
NO
YES
S706
NAPT/PFエントリ削除
S707
エンド

【図８】


サーバ
907
ローカルネットワーク
903
ディレクトリサービスサーバ
901
ディレクトリデータベース
906
ファイアウォール兼中継サーバプログラム
905
ファイアウォール
904
インターネット
900
クライアント
902