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

特許第4524906号
(P4524906)

(45)発行日　平成22年8月18日(2010.8.18)　(24)登録日　平成22年6月11日(2010.6.11)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	Z
G06F 13/00	(2006.01)	G06F	13/00	351Z
H04L 29/08	(2006.01)	G06F	13/00	353C
		H04L	13/00	307A

請求項の数 10　(全 20 頁)

(21)出願番号　特願2000-337392 (P2000-337392)
(22)出願日　平成12年11月6日 (2000.11.6)
(65)公開番号　特開2002-141953 (P2002-141953A)
(43)公開日　平成14年5月17日 (2002.5.17)
審査請求日　平成19年3月5日 (2007.3.5)

(73)特許権者　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100101801
弁理士　山田　英治
(74)代理人　100093241
弁理士　宮田　正昭
(74)代理人　100086531
弁理士　澤田　俊夫
(72)発明者　浅井　伸昌
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

審査官　安藤　一道

最終頁に続く

(54)【発明の名称】通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体

(57)【特許請求の範囲】

【請求項１】

外部ネットワークとローカルネットワークとの中継手段として機能する通信中継装置であり、

前記ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記提供サービスの各々に対応して固有のアクセス情報の設定を行い、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示する処理を実行する構成を有し、

前記サービスに対するアクセス情報は、

前記提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号である

ことを特徴とする通信中継装置。

【請求項２】

前記通信中継装置は、

前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を定期的に前記内部端末から受信し、サービス提供可否の状態情報に基づいて端末管理データを更新し、更新した端末管理データに基づいて、外部ネットワークに対して提示するサービス情報とアクセス情報の更新を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。

【請求項３】
前記通信中継装置は、
外部ネットワークを介したクライアントからの前記内部端末に対するアクセス要求に応答して、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号を前記クライアントに提供するとともに、前記クライアントからの外部ポート番号を用いたアクセス要求に応じて、外部ポート番号から内部ポート番号への変換処理を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項４】
前記通信中継装置は、
ａ．該中継装置のグローバルＩＰアドレス、
ｂ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号、
ｃ．前記内部端末の個々に設定されたプライベートＩＰアドレス、
ｄ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号、
とを対応付けたネットワークアドレス変換テーブルを有し、
前記通信中継装置は、
前記ネットワークアドレス変換テーブルに基づいて、外部ネットワークを介した内部端末へのアクセス要求中に含まれる中継装置のグローバルＩＰアドレスと外部ポート番号から、プライベートＩＰアドレスと内部ポート番号への変換を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項５】
前記通信中継装置は、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントの認証を実行し、認証成立を条件として、前記サービス情報と、該サービスに対するアクセス情報を提示する処理を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項６】
前記通信中継装置は、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントのアドレスを設定したファイアウォールを構築して、ファイアウォールに基づくアクセス制限処理を実行する構成を有することを特徴とする請求項１に記載の通信中継装置。
【請求項７】
外部ネットワークとローカルネットワークとの中継手段として機能する通信中継方法であり、
前記ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記内部端末の提供サービスの各々に対応して固有のアクセス情報の設定を行うステップと、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号である前記サービスに対するアクセス情報を提示するステップと、
を有することを特徴とする通信中継方法。
【請求項８】
ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記提供サービスの各々に対応して固有のアクセス情報の設定を行い、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示する処理を実行する構成を有し、前記サービスに対するアクセス情報

は、前記提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号として、前記外部ネットワークと前記ローカルネットワークとの中継手段として機能する通信中継装置の管理する前記ローカルネットワークに接続された通信端末装置において、

該通信端末装置は、前記提供可能なサービスを示すサービス情報を、サービス識別データとサービスに対応する前記内部ポート番号を含む構成として前記通信中継装置に登録することを特徴とする通信端末装置。

【請求項９】

前記通信端末装置は、

前記通信中継装置からの要求に応じて、サービス提供可否の状態情報を送信する構成を有することを特徴とする請求項８に記載の通信端末装置。

【請求項１０】

外部ネットワークとローカルネットワークとの中継手段として機能する通信中継システムにおけるデータ通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム記憶媒体であって、前記コンピュータ・プログラムは、

前記ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記内部端末の提供サービスの各々に対応して固有のアクセス情報の設定を行うステップと、

外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号である前記サービスに対するアクセス情報とを提示するステップと、

を実行することを特徴とするプログラム記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体に関する。さらに詳細には、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て、双方からの１対１のアクセスを可能とする通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体に関する。

【０００２】

【従来の技術】

現在、爆発的に普及しているインターネットではルーティテングプロトコルとしてＩＰ(Ｉnternet Ｐrotocol）が用いられている。現在使用されているＩＰはＩＰｖ４であり、発信元／宛先として３２ビットからなるアドレス（ＩＰアドレス）が用いられている。インターネット通信においては、３２ビットＩＰアドレスを各発信元／宛先にユニークに割り当てるグローバルＩＰアドレスを採用し、ＩＰアドレスに応じて、個々の発信元／宛先を判別している。しかし、インターネットの世界は急速に広がりを見せており、ＩＰｖ４の限られたアドレス空間、すなわちグローバルアドレスの枯渇が問題となってきている。これを解決するためにＩＥＴＦ（Internet Engineering Task Force）では、次世代ＩＰアドレスとしてＩＰアドレス空間を３２ビットから１２８ビットに拡張する新しいＩＰｖ６を提案している。しかし、ＩＰｖ６への移行には時間を要し、即効性のある対応にはなり難い。

【０００３】

現在のＩＰｖ４を用いながらアドレス空間を広げる手法として、プライベートアドレスを用いる方法が提案されている。プライベートアドレスはグローバルアドレスと異なり、一定の組織内で使用されるアドレスである。例えば、ある企業組織内で任意の数のプライベートアドレスを設定して、個々の社員端末にプライベートアドレスを割り当てることができる。このプライベートアドレスを用いた場合は、外部との接続の際にグローバルＩＰアドレスに変換することが必要となる。それを実現する装置としてＮＡＴ(Network Addre

ss Ｔranslator）がある。

【０００４】

例えば、１つのグローバルＩＰアドレスをＩＳＰ（Internet Service Provider）からもらい、ＬＡＮ内部をＤＨＣＰ（Dynamic Host Configuration Protocol）サーバによってプライベートＩＰアドレスで管理する方法がある。この方式はＬＡＮ(Local Area Network)内部からＷＡＮ（Wide Area Network）へパケットを送出する際、ＳＯＨＯルータでＩＰヘッダのソース（ｓｒｃ）アドレスをＳＯＨＯルータの持つグローバルＩＰアドレスに変換する方法であり、ベーシックＮＡＴと呼ばれる。図１にベーシックＮＡＴ方式を使用したシステムを説明する図を示す。図１において、例えば企業内のプライベートアドレスの割り当てられた端末、ＴＣＰ／ＩＰ（Transmission Control Protocol／Internet Protocol）接続端末１０１～１０ｎがあり、各端末はＬＡＮ１２０によってＮＡＴ１３０に接続される。ＮＡＴ１３０は、インターネット１４０に接続され、各端末１０１～１０ｎのＩＰアドレスはＮＡＴ１３０によってグローバルアドレスに変換される。

【０００５】

ＩＰアドレスの表記は３２ビットのアドレスを８ビットを単位として１０進数で表して表記する。ＮＡＴ１３０は接続端末１０１～１０ｎからのパケットに対し、予め設定されている数のグローバルアドレスを先着順に割り当てる。従ってグローバルアドレス設定数以上の通信は並列に実行できないことになる。従って、あくまで並列に実行可能な通信数はグローバルアドレスの数によって制限されてしまう。このようにＮＡＴでは１つのプライベートアドレスに対して１つのグローバルアドレスを対応させる処理をしているので、根本的なアドレス枯渇問題を解決するものとはなっていない。

【０００６】

グローバルＩＰアドレスをさらに節約するために１個のグローバルＩＰアドレスの異なるＴＣＰポートを用いて複数のプライベートＩＰアドレスに対応させる技術も用いられることがある。ＬＡＮ内部の複数のＩＰ端末からＷＡＮ側へパケットを同時に送信出来るように、ＳＯＨＯルータでｓｒｃアドレスに加えてソース（ｓｒｃ）ポートの変換も行い、ＷＡＮ側からの戻りのパケットをそのｓｒｃポートを見てプライベートＩＰアドレスに変換する拡張ＮＡＴ、通称、ＩＰマスカレードという方法である。

【０００７】

ＩＰマスカレードを用いた通信システム構成を図２に示す。図２においては、インターネット２０１側にグローバルアドレスが１つあり、例えば企業内のプライベートアドレスの割り当てられた端末であるＴＣＰ／ＩＰ接続端末が、ＵＤＰ（User Datagram Protocol）で規定されているポート番号によって識別可能であるとき、ＴＣＰやＵＤＰのポート番号を利用することによってそれぞれの端末個々が、１つの共通のグローバルアドレスを利用して通信を実行する構成としたものである。

【０００８】

ＩＰマスカレードにより、複数の端末からＷＡＮ側の同一端末に同時アクセスすることが可能になるが、この方法では最初にＬＡＮ側の端末からＷＡＮ側の端末へセッションを張らないと、ＷＡＮ側からＬＡＮ内部へのデータ通信が出来ない。ＮＡＴを使用して、ＷＡＮ側から最初にＬＡＮ側に対してデータ通信を行う方法は、現在提案されていない。さらにいえば、ＬＡＮ側からＷＡＮ側へどのようなサービスが可能であるかについての情報を提供する手段がない。アノニマス（Ａｎｏｎｙｍｏｕｓ）ＦＴＰサーバなどをＬＡＮ内に立ち上げる例もあるが、このためにはＮＡＴにおけるマッピング処理構成を手動で事前に設定しておかなければならない。また、ＷＡＮ側からアクセスを行なうクライアントもそのサーバの存在を事前に知っておく必要がある。

【０００９】

【発明が解決しようとする課題】

本発明は、上述のような従来技術の欠点に鑑みてなされたものであり、グローバルアドレスで管理されているＷＡＮ側から、プライベートアドレス管理下の登録サービスを利用可能にする通信中継装置、通信中継方法、および通信端末装置、並びにプログラム記憶媒体

を提供することを目的とする。

【００１０】

【課題を解決するための手段】

本発明の第１の側面は、

外部ネットワークとローカルネットワークとの中継手段として機能する通信中継装置であり、

前記ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記提供サービスの各々に対応して固有のアクセス情報の設定を行い、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示する処理を実行する構成を有し、

前記サービスに対するアクセス情報は、

前記提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号であることを特徴とする通信中継装置にある。

【００１２】

さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、前記ローカルネットワークに接続された内部端末の提供可能なサービス情報を定期的に前記内部端末から受信し、サービス提供可否の状態情報に基づいて端末管理データを更新し、更新した端末管理データに基づいて、外部ネットワークに対して提示するサービス情報とアクセス情報の更新を実行する構成を有することを特徴とする。

【００１３】

さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、外部ネットワークを介したクライアントからの前記内部端末に対するアクセス要求に応答して、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号を前記クライアントに提供するとともに、前記クライアントからの外部ポート番号を用いたアクセス要求に応じて、外部ポート番号から内部ポート番号への変換処理を実行する構成を有することを特徴とする。

【００１４】

さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、ａ．該中継装置のグローバルＩＰアドレス、ｂ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して、該内部ポート番号とは異なる値に設定された外部ポート番号、ｃ．前記内部端末の個々に設定されたプライベートＩＰアドレス、ｄ．前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号、とを対応付けたネットワークアドレス変換テーブルを有し、前記通信中継装置は、前記ネットワークアドレス変換テーブルに基づいて、外部ネットワークを介した内部端末へのアクセス要求中に含まれる中継装置のグローバルＩＰアドレスと外部ポート番号から、プライベートＩＰアドレスと内部ポート番号への変換を実行する構成を有することを特徴とする。

【００１５】

さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントの認証を実行し、認証成立を条件として、前記サービス情報と、該サービスに対するアクセス情報を提示する処理を実行する構成を有することを特徴とする。

【００１６】

さらに、本発明の通信中継装置の一実施態様において、前記通信中継装置は、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、アクセス要求クライアントのアドレスを設定したファイアウォールを構築して、ファイアウォールに基づくアクセス制限処理を実行する構成を有することを特徴とする。

【００１７】

さらに、本発明の第２の側面は、
外部ネットワークとローカルネットワークとの中継手段として機能する通信中継方法であり、
前記ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記内部端末の提供サービスの各々に対応して固有のアクセス情報の設定を行うステップと、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号である前記サービスに対するアクセス情報を提示するステップと、
を有することを特徴とする通信中継方法にある。

【００２４】

さらに、本発明の第３の側面は、ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記提供サービスの各々に対応して固有のアクセス情報の設定を行い、外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、該サービスに対するアクセス情報とを提示する処理を実行する構成を有し、前記サービスに対するアクセス情報は、前記提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号として、前記外部ネットワークと前記ローカルネットワークとの中継手段として機能する通信中継装置の管理する前記ローカルネットワークに接続された通信端末装置において、
該通信端末装置は、前記提供可能なサービスを示すサービス情報を、サービス識別データとサービスに対応する前記内部ポート番号を含む構成として前記通信中継装置に登録することを特徴とする通信端末装置にある。

【００２６】

さらに、本発明の通信端末装置の一実施態様において、前記通信端末装置は、前記通信中継装置からの要求に応じて、サービス提供可否の状態情報を出力する構成を有することを特徴とする。

【００２７】

さらに、本発明の第４の側面は、
外部ネットワークとローカルネットワークとの中継手段として機能する通信中継システムにおけるデータ通信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム記憶媒体であって、前記コンピュータ・プログラムは、
前記ローカルネットワークに接続された内部端末と該内部端末に接続された下位の階層の機器で提供可能なサービスを示すサービス情報を取得して内部端末別に管理し、前記内部端末の提供サービスの各々に対応して固有のアクセス情報の設定を行うステップと、
外部ネットワークからの前記内部端末に対するアクセス要求に応答して、前記サービス情報と、前記内部端末の提供サービスの各々に対応して固有に設定された内部ポート番号に対応して設定された情報であり、該内部ポート番号とは異なる値に設定された外部ポート番号である前記サービスに対するアクセス情報とを提示するステップと、
を実行することを特徴とするプログラム記憶媒体にある。

【００２８】

なお、本発明の第４の側面に係るプログラム記憶媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。

【００２９】

このようなプログラム記憶媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと記憶媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該記憶媒体を介してコンピュー

タ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３０】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３１】

【発明の実施の形態】

［１．システム概要］

図３に本発明の通信中継装置および通信端末装置によって構成されるシステムの概要を説明する図を示す。図３は、ＷＡＮ環境としてのインターネットとＬＡＮ環境下の例えばＳＯＨＯ（Small Office/Home Office）とを、通信中継装置であるネットワーク接続機器としてのルータ（ＳＯＨＯルータ）により相互接続した環境、すなわち、インターネットにＩＰ接続されたＳＯＨＯ環境の例である。なお、ここでは、ルータをネットワーク相互間の接続機器の例として説明するが、ゲートウェイその他のネットワーク接続機器も以下の説明と同様の構成を持つ機器として利用可能である。

【００３２】

図３に示すように各家庭、Ａさん宅、Ｂさん宅、あるいはその他、各事業所にはインターネット接続された、通信中継装置としてのＳＯＨＯルータ３１０，３２０が各々１台設置されている。そのＳＯＨＯルータはＩＳＰ（Internet Service Provider）などからグローバルＩＰアドレス（ＩＰｖ４）を１つ、もしくは複数個、付与され、その管理下に通信端末装置として複数のＩＰ端末（ＰＣ，モバイル端末など）を管理する。図３では、Ａさん宅のＳＯＨＯルータ３１０に、ＩＰ端末１，３１１とＩＰ端末２，３１２が接続され、Ｂさん宅のＳＯＨＯルータにＩＰ端末としてＨＴＴＰサーバ３２１、ＦＴＰサーバ３２２、ＲＴＳＰサーバ３２３が接続された例を示している。

【００３３】

図３の例では、Ａさん宅のＳＯＨＯルータ３１０にはグローバルＩＰアドレス［４３．１１．ＸＸ．ＸＸ］が設定され、Ｂさん宅のＳＯＨＯルータ３２０にはグローバルＩＰアドレス［４３．１０．ＸＸ．ＸＸ］が設定されている。ここで、ＳＯＨＯルータは、アクセス要求の各ホストに動的にＩＰアドレスを割り当てるＤＨＣＰ（Dynamic Host Configuration Protocol）サーバの機能と、ドメイン名とＩＰアドレスとの対応付け処理を実行するＤＮＳ（Domain NameSystem）サーバとしての機能を兼務する。各ＳＯＨＯルータ３１０，３２０の管理下のＩＰ端末は、ＳＯＨＯルータにより割り当てられるＩＰアドレスによってルーター、インターネットを介した外部端末との接続が可能となり、様々な処理、例えばメール転送、画像転送などが可能となる。

【００３４】

ＳＯＨＯルータ３１０，３２０は、ＩＰ端末接続時にそのプライベートＩＰアドレスを管理下の各端末３１１，３１２，３２１，３２２，３２３に割り振り、その名前を登録する。各ＳＯＨＯルータ管理下のＩＰ端末では、ＦＴＰ(File Transfer Protocol)、ＨＴＴＰ（Hyper Text Transfer Protocol）、ＲＴＳＰ(Real-time Streaming Protocol)などのサービスを提供することができる。

【００３５】

図３の例では、Ａさん宅のＳＯＨＯルータ３１０は、管理下のＩＰ端末にプライベートＩＰアドレスとして、ＩＰ端末１，３１１に［１９２．１６８．０．２］、ＩＰ端末２，３１２に［１９２．１６８．０．３］を設定し、Ｂさん宅のＳＯＨＯルータ３２０は、管理下のＩＰ端末にプライベートＩＰアドレスとして、ＨＴＴＰサーバ３２１に［１９２．１６８．０．２］、ＦＴＰサーバ３２２に［１９２．１６８．０．３］、ＲＴＳＰサーバ３２３に［１９２．１６８．０．４］を設定している。

【００３６】

［２．サービス登録］

本発明の通信中継装置であるネットワーク接続機器としての図３の構成におけるＳＯＨＯルータ３１０，３２０は、各ＳＯＨＯルータ管理下のＩＰ端末３１１，３１２、３２１，３２２，３２３のＳＯＨＯルータ接続時に、その端末で現在提供可能なサービスをＳＯＨＯルータ上のサービスアクセス機器リスト管理デーモン（以下、省略してＳＡＬｄ（Service Access Device List Demon）と呼ぶ）に登録する。なお、デーモンとは、システム常駐プログラムであり、アプリケーション・プログラム、またはシステムの状態に応じて自動的に特定の処理を実行するプログラムである。

【００３７】

本発明の通信中継装置であるネットワーク接続機器（ｅｘ．ルータ、ゲートウェイなど）に設定されるＳＡＬｄは、ＳＯＨＯ環境において各ＩＰ端末の提供できるサービスを階層的に管理したり、そのサービス内容を動的に更新したり、それをＷＡＮ側に提示する処理を実行するプログラムである。

【００３８】

一方、ＳＡＬｄのを有するネットワーク接続機器の管理下のＩＰ端末には、サービス監視デーモン（ＳＡＬｄクライアント、略してＳＡＬｄｃと呼ぶ）が設定されている。ＳＯＨＯルータ等のネットワーク接続機器のＳＡＬｄは各ＩＰ端末上のサービス監視デーモン（ＳＡＬｄｃ）からサービス登録メッセージ（ＲＥＧＩＳＴＥＲ）をネットワーク接続、あるいはＩＰ端末の電源投入時に受け取る。ＳＡＬｄは内部管理下のすべてのＳＡＬｄｃからのサービス登録メッセージ（ＲＥＧＩＳＴＥＲ）を受け取り、それを端末別に階層的に管理する。

【００３９】

ＳＯＨＯ環境のＬＡＮ側のプライベートＩＰアドレスを使用した端末のサービスの階層的管理の例としては、例えば、ＬＡＮ内にアプリケーションゲートウェイなどの機能を持つＰＣがいて、そのＰＣの管理下に非ＩＰ機器（例えば１３９４、ＵＳＢなどの独自データリンクをもつ）が接続された環境における機器の管理の場合などがある。図４に階層構成を持つ機器接続システム例を示す。

【００４０】

図４のシステムは、インターネットにネットワーク接続機器としてのＳＯＨＯルータ４０１が接続され、その下位にＩＰ端末としてのＰＣ１，４０２，アプリケーションゲートウェイ機能を持つＰＣ２，４０３が接続され、ＰＣ２，４０３の下位に非ＩＰ端末として、１３９４パスに接続されたカメラ４０４，デッキ４０５、さらにＵＳＢ接続機器４０６が接続された構成である。

【００４１】

非ＩＰ機器が行うサービスは、ＩＰ端末のＰＣ２，４０３の下の階層の機器のサービスであり、例えば１３９４のＤＶカメラなどの映像サービス、デッキの映像サービス等である。ネットワーク接続機器としてのＳＯＨＯルータ４０１は、ＩＰ端末、非ＩＰ端末の提供サービスを登録して階層的管理を行なうことができる。

【００４２】

図５に１つのＩＰ端末上に複数のサービスが存在する場合の、サービス登録の方法を示す。図５は、図３におけるＡさん宅のシステム構成を示している。ＩＰ端末１，３１１ではＦＴＰ(File Transfer Protocol)、ＨＴＴＰ（Hyper Text Transfer Protocol）、何かしらのその端末独自なサービスが起動されており、端末２，３１２ではＨＴＴＰ、ＲＴＳＰ(Real-time Streaming Protocol)のサービスが起動されているとする。

【００４３】

ＩＰ端末１，３１１は、サービス監視デーモン（ＳＡＬｄｃ）の監視により、起動中のサービス（アプリケーション）情報を取得して、＜サービス名、内部ポート番号＞として、｛＜ＦＴＰ，２０＞、＜ＨＴＴＰ，８０＞、＜独自サービス、６００１＞を得ており、また、ＩＰ端末２，３１２では｛＜ＨＴＴＰ，８０＞、＜ＲＴＳＰ，５５４＞｝を取得している。各ＩＰ端末は、これらの起動サービス（アプリケーション）情報をそれぞれ、ネットワーク接続機器（ＳＯＨＯルータ）のＳＡＬｄにＲＥＧＩＳＴＥＲ（登録）する。

【００４４】
ＩＰ端末１，３１１の、サービス監視デーモン（ＳＡＬｄｃ１）からＳＯＨＯルータ３１０に送信される登録メッセージ（ＲＥＧＩＳＴＥＲ）例を図６に示す。
【００４５】
図６に示すように、登録メッセージは、端末に割り当てられたプライベートＩＰアドレス、端末名、端末属性、サービス名、サービス属性、内部ポート番号によって構成される。プライベートＩＰアドレスは、ＳＯＨＯルータ３１０によって付与されたＩＰアドレスである。端末名は、ＳＯＨＯルータ３１０管理下の各端末を識別する識別名であり、端末属性は、ＰＣ（Personal Computer）などの機器の種別を示す。インターネット接続可能な例えばテレビ、ビデオ、サーバ、その他家電製品などＩＰアドレスの設定により通信可能な機器の種類を示すデータである。サービス名は、ＩＰ端末において提供するサービス（アプリケーション）を示している。図６の例では、ＩＰ端末１，３１１は、ＦＴＰ(File Transfer Protocol)、ＨＴＴＰ（Hyper Text Transfer Protocol）、その他の独自サービスを提供可能なＰＣである。サービス属性は、ＦＴＰ，ＨＴＴＰ，独自サービスのサービスの態様を示している。内部ポート番号は、各サービスを識別するための番号として、各サービスに対して設定された番号である。
【００４６】
ネットワーク接続機器（ｅｘ．ルータ、ゲートウェイなど）のＳＡＬｄは、図６に示すような登録メッセージを受領して、管理データ（図８参照）として登録する。
【００４７】
［３．サービスの更新］
ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄは、管理下ＩＰ端末の各ＳＡＬｄｃとの間で、定期的なサービスの情報交換を行い、ＩＰ端末の提供サービスの内容を更新する。ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄは管理下ＩＰ端末のＳＡＬｄｃに対して、管理下ＩＰ端末の管理データに登録済みのサービスが有効に利用可能であるかのチェックを定期的、例えば３０秒単位で行なう。
【００４８】
ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄは、管理下ＩＰ端末のサービスアクセス機器リストに登録済みのサービス内容を示すメッセージ（ＫＥＥＰ ＡＬＩＶＥ）を送信し、管理下ＩＰ端末のＳＡＬｄｃはメッセージ（ＫＥＥＰ ＡＬＩＶＥ）を受信し、そのサービスが端末側で提供可能であればＡＣＫを返す。ＳＡＬｄは所定時間までこのＡＣＫを待って、受信できない場合はその内容をサービスアクセス機器リストから削除する。また、ＳＡＬｄｃはＩＰ端末で新たに起動されたサービスを監視し、ＳＡＬｄにＲＥＧＩＳＴＥＲメッセージを送信する。
【００４９】
［４．ＮＡＴへのサービスマッピング］
ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄは管理下のＩＰ端末の提供可能な各種サービス内容をＷＡＮ側のクライアントに提示するためのサービスマッピングを行う。ＬＡＮ側の各ＩＰ端末は、プライベートＩＰアドレスで管理されているため、ＷＡＮ側から各ＩＰ端末を直接アクセスすることができない。従って、ＬＡＮ内の接続ＩＰ端末で提供するサービスをＷＡＮ側クライアントがＬＡＮ内の接続ＩＰ端末に直接問い合わせを行なうことはできない。
【００５０】
ＷＡＮ側クライアントがＬＡＮ内の接続ＩＰ端末の提供サービスを知り、サービスを実行させるためには、ＩＰ端末を管理するネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）に割り当てられたグローバルＩＰアドレスから、対応するＩＰ端末のプライベートアドレスに変換させる必要がある。各ＩＰ端末では、図６の登録メッセージの例で示したように、ＦＴＰ，ＨＴＴＰ…など、複数のサービスを提供する可能性があるので、ＩＰアドレスだけではなく、各サービスのポート番号情報も必要である。
【００５１】

ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄでは管理下ＩＰ端末の提供するサービスに対応するＷＡＮ側に見せる外部ポートを決定し、ＳＯＨＯルータのグローバルＩＰアドレス、外部ポート宛てに到達したパケットのＩＰヘッダの宛先アドレス／ポート番号（ｄｅｓｔｉｎａｔｉｏｎ ａｄｄｒｅｓｓ／ｐｏｒｔ）を、各ＩＰ端末のプライベートＩＰアドレス、サービスの内部ポート番号に書き換える様、ＮＡＴ(Network Address Translator)に設定する。ＮＡＴに設定する変換テーブルの例を図７に示す。

【００５２】

図７の例は、図５のシステムにおけるＳＯＨＯルータ３１０に設定される変換テーブルの例である。図７に示すように、ＮＡＴ変換テーブルには、変換前宛先ＩＰアドレス、変換前宛先ポート番号、変換後宛先ＩＰアドレス、変換後宛先ポート番号が設定される。

【００５３】

変換後宛先ＩＰアドレスは、ネットワーク接続機器（ＳＯＨＯルータ）３１０がＩＰ端末１，３１１、およびＩＰ端末２，３１２に割り当てているプライベートＩＰアドレスであり、また、変換後ポート番号は、各ＩＰ端末の提供サービスに対応付けられた内部ポート番号である。これらは、先に説明した図６の登録メッセージに基づくリストから取得できる。

【００５４】

変換前宛先ＩＰアドレスは、ＳＯＨＯルータ３１０のグローバルＩＰアドレスである。変換前宛先ポート番号は、ＳＯＨＯルータ３１０の管理ＩＰ端末の提供するサービス毎にＳＯＨＯルータが設定する外部ポート番号である。

【００５５】

ネットワーク接続機器としてのＳＯＨＯルータのＮＡＴ、ＳＡＬｄとの処理について具体的に説明する。ＳＯＨＯルータのＳＡＬｄは、内部データとして、図８に示す端末管理データを持つ。

【００５６】

図８の例は、図５のシステムにおけるＳＯＨＯルータ３１０に設定される端末管理データの例である。図８の端末管理データには、端末に割り当てられたプライベートＩＰアドレス、端末名、端末属性、サービス名、サービス属性、外部ポート番号、内部ポート番号によって構成される。これらのデータは、先に図６を用いて説明した各管理ＩＰ端末からの登録メッセージに基づいて生成される。

【００５７】

プライベートＩＰアドレスは、ＳＯＨＯルータ３１０によって付与されたＩＰアドレスである。端末名は、ＳＯＨＯルータ３１０管理下の各端末を識別する識別名であり、端末属性は、ＰＣ（Personal Computer）などの機器の種別を示す。サービス名は、ＩＰ端末において提供するサービス（アプリケーション）を示している。サービス属性は、ＦＴＰ，ＨＴＴＰ，独自サービスのサービスの態様を示している。外部ポート番号は、ＷＡＮ側クライアントに提示スルために、ＳＯＨＯルータで決めたサービスを識別する番号である。内部ポート番号は、各サービスを識別するための番号として、各サービスに対して設定された番号である。

【００５８】

この例では、ＩＰ端末１，３１１のＦＴＰ、ＨＴＴＰ、独自サービスに対して、外部ポートアドレスがそれぞれ８０００、８００１、８００２が割り当てられており、同様にＩＰ端末２，３１２のＨＴＴＰ、ＲＴＳＰに対して、外部ポートアドレスがそれぞれ８００３、８００４が割り当てられている。この外部に割り当てるポート番号は、カーネルなどが使用しない領域をＳＡＬｄが自由に設定できるものとし、サービスが終了した場合などはこのポート番号はプール領域に戻される。また、サービスによっては（例えばメッセージペイロード内にサービスの提供ポート番号など埋め込むＲＴＳＰやＦＴＰなど）、外部からの接続先である外部ポートを指定してＲＥＧＩＳＴＥＲすることができる。これにより、ＮＡＴ変換前のポート番号が指定でき、事前にＲＴＳＰなどのメッセージペイロードにその指定したポート番号を埋め込むことが出来る。

【００５９】
［５．サービスアクセス機器リスト］
ネットワーク接続機器としてのＳＯＨＯルータのＳＡＬｄは図８に示す端末管理データを保持し、ＷＡＮ側にいるクライアントからそのＳＯＨＯルータの管理ＩＰ端末に対するサービス要求があった場合、図９に示すようなサービスアクセス機器リストを返す。
【００６０】
図９に示すように、サービスアクセス機器リストには、ネットワーク接続機器としてのＳＯＨＯルータの管理するＩＰ端末情報として、端末名、端末属性、サービス名、サービス属性が含まれる。
【００６１】
サービスアクセス機器リストには、上述のようにそのＳＯＨＯ環境内にある端末の名前、その端末の属性、サービス名、そのサービスの属性などの項目が含まれる。ＷＡＮ側にいるユーザにどのようなネットワーク機器が存在し、その上でどのようなサービスが稼動しいるかを知らしめるためである。また、サービスアクセス機器リスト作成時に、ＮＡＴによるアドレス変換は設定するが、まだこの時点では、ＷＡＮ側からの各種サービスに対するファイアウォールの設定を禁止しておく。
【００６２】
ＷＡＮ側クライアントは、図９に示すサービスアクセス機器リストから、サービスを選択し、選択サービスをネットワーク接続機器としてのＳＯＨＯルータに通知し、ＳＯＨＯルータは、選択サービスに対応する外部ポート番号を要求クライアントに提供する。ＳＯＨＯルータ３１０は、ＷＡＮ側クライアントのグローバルＩＰアドレスと外部ポート番号（変換前宛先ポート番号）に基づくアクセス要求を図７のＮＡＴ変換テーブルに基づいて、ＩＰ端末のプライベートＩＰアドレスと、変換後ポート番号に変換する。
【００６３】
なお、サービスアクセス機器リストは、ＷＡＮ側にいる認証されたユーザに対してのみ提示する構成とするのが望ましい。また、認証されたユーザをユーザ登録データとして保持し、ユーザ毎に全てのサービス情報を表示したり、特定のサービスのみを抜き出して、特定の端末の情報だけを収集して、ユーザ固有のサービスアクセス機器リストを生成して提示する構成としてもよい。
【００６４】
［６．ＳＡＬｄの処理］
ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄの実行するサービス登録フローを図１０に示す。まず、定期的に発行されるＳＡＬｄイベントを取得（Ｓ１０１）すると、管理下のＩＰ端末からの新規サービス登録メッセージがあるか否かを検証（Ｓ１０２）し、ある場合は、登録メッセージに対する外部ポートを設定（Ｓ１０３）し、ＮＡＴ変換テーブルを設定する。これは、図７のテーブルを生成する処理である。
【００６５】
ＮＡＴ変換テーブルの設定が成功すると、登録完了通知をＩＰ端末に送信（Ｓ１０５）し、登録ＩＤを決定し、サービスの監視処理イベントをタイマー管理を開始（Ｓ１０６）し、端末管理データ（図８参照）を生成（Ｓ１０７）する。ＮＡＴ変換テーブルの生成に失敗した場合は、登録失敗を送信し（Ｓ１０８）、フローの先頭に戻る。
【００６６】
ステップＳ１０２において、新規サービス登録処理でないと判定した場合は、サービス登録ＩＰ端末に対するサービスの提供可否の問い合わせとして実行される［ＫＥＥＰ　ＡＬＩＶＥ］に対する応答［ＡＣＫ］の受信であるかを判定（Ｓ１０９）する。ＩＰ端末は、サービス提供可否の状態情報としてサービス提供可である場合はＡＣＫを出力する。ネットワーク接続機器のＳＡＬｄは、ＩＰ端末からＡＣＫ受信をした場合は、登録サービスに対するＡＣＫであるか否かを検証（Ｓ１１０）し、登録サービスである場合は、タイマーのリセット（Ｓ１１１）を行なう。登録サービスに対するＡＣＫでない場合は、無効（Ｓ１１２）として扱う。

【００６７】
ステップＳ１０９において、［ＫＥＥＰ　ＡＬＩＶＥ］に対する応答［ＡＣＫ］の受信でないと判定されると、タイマーイベントであるか否かが判定（Ｓ１１３）され、タイマーイベントである場合は、図１１のタイマー処理（Ｓ１１４）が実行される。
【００６８】
図１１のタイマーイベント処理について説明する。まずタイマーが０であるか否かが判定（Ｓ２０２）され、０である場合は、登録ＩＰ端末に対するサービスの提供可否の問い合わせとして実行される［ＫＥＥＰ　ＡＬＩＶＥ］をＩＰ端末に送信（Ｓ２０３）する。次に、タイマーが予め定めたＩＰ端末からのＡＣＫ応答待機時間を超えたか否かを判定（Ｓ２０４）し、超えた場合には、ネットワーク接続機器（ｅｘ．ルータ，ゲートウェイ）のＳＡＬｄの管理する端末管理データ（図８参照）から、登録サービスを削除（Ｓ２０５）し、タイマーを更新（Ｓ２０６）する。なお、図１１でのタイマーイベントは、登録ＩＰ端末に対するサービスの提供可否の問い合わせとして実行される［ＫＥＥＰ　ＡＬＩＶＥ］発行処理で起動する周期割り込みイベントである。
【００６９】
［７．ユーザ認証］
ＳＡＬｄは、ネットワーク接続機器（ｅｘ．ＳＯＨＯルータ）のある予約ポートとしてのウェルノウンポート（Ｗｅｌｌ　Ｋｎｏｗｎ　Ｐｏｒｔ）にＴＣＰ／ＵＤＰコネクトするデーモンである。従って、ＳＯＨＯルータのアドレス（グローバルＩＰアドレス）とそのポート番号が知られてしまえば、ＷＡＮ側のいかなる悪意をもったユーザからもアクセスできてしまう。しかし、図９用いて説明したサービスアクセス機器リストに関しては、ＳＯＨＯ環境内の個人もしくは事業主の秘密情報である。ましては外部からそのネットワーク機器にアクセスでき、コントロールされてしまうのはもっての他である。
【００７０】
従って、本システムにおいては、ＷＡＮ側クライアントからネットワーク接続機器（ｅｘ．ＳＯＨＯルータ）のＳＡＬｄに対するアクセス時に認証を実行する。具体的には、ＨＴＴＰｄ（ＨＴＴＰデーモン）などが実装しているユーザ、パスワードによる認証を使用し、ＳＡＬｄアクセス時にＣＧＩ（Common Gateway Interface）などを使用し、ＨＴＴＰｄサーバが認証を行うディレクトリ以下にアクセスするように構成する。このディレクトリでの認証を事前に登録してあるユーザ名、パスワードにて行い、許可されたユーザに対してのみ、サービスアクセス機器リストを提供する構成とする。
【００７１】
従って、ユーザ認証を行なうネットワーク接続機器としての例えばＳＯＨＯルータの管理下のＩＰ端末に接続するためには、ＳＯＨＯルータに対するユーザ登録を必要とする。なお、フリーなアクセスを許容する環境であれば必ずしもユーザ登録、認証処理を実行する必要はない。
【００７２】
［８．サービスの選択、ファイアフォールの設定］
ＷＡＮ側にいる認証されたユーザは、ＨＴＴＰなどを拡張したプロトコルを使用してＳＡＬｄからサービスアクセス機器リスト（図９参照）を取得することができる。このリストはＨＴＭＬなどを使用して書かれており、ユーザはその中から指定したサービス項目を選択することができる。ＳＡＬｄがユーザの指定したサービス項目を受け取った時点で、ＳＯＨＯルータ内のファイアフォールに対して、そのユーザからのセッションの送信元（ｓｒｃ）ＩＰアドレス（および送信元（ｓｒｃ）ポート番号）と、ネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）の提供するサービスアクセス機器リストにより指定したサービスに対応する宛先ポート番号（外部ポート番号）の組み合わせで、その通信に対してのアクセスを許可する。例えば、ＷＡＮ側にいるクライアント（ＩＰアドレスが43.10.133.89）が図９に示すサービスアクセス機器リストのうち、ＩＰ端末１のＦＴＰサービスを選択したとすると、図１２に示すようなファイアウォールの設定が可能となる。なお、４３．１１．１３５．８７はＳＯＨＯルータのグローバルＩＰアドレスとする。

【００７３】
図１２のファイアウォールは、送信元ＩＰアドレスが［43.10.133.89］のユーザに対して外部ポート番号８０００のサービス、すなわち、図８に示す管理データから理解されるように、ＩＰ端末１のＦＴＰサービスを許可するファイアウォールである。
【００７４】
ちなみにファイアフォールの設定は、ＷＡＮ側からＬＡＮ側への通信は、原則として事前に禁止しておく。これにより、認証されたユーザの選択したサービスに対して、そのユーザの属する端末（場合によってはセッション）からのアクセスしか許可しないことになり、ＳＯＨＯ環境内の機器に対する外部からのアクセスに対するセキュリティを強化することができる。
【００７５】
このように、本発明のシステムではＷＡＮ側にいる認証されたユーザがサービスを選択した時点で、ＳＯＨＯルータ内にあるファイアフォールに対して、選択したユーザの端末ＩＰアドレス、ＳＯＨＯルータのグローバルＩＰアドレス、サービスへの外部ポート番号の組を設定してアクセスを許可する構成とした。従って、外部クライアントは、ＳＯＨＯのＬＡＮ内の機器に対するルータの許可のない制御は不可能であり、高度なセキュリティ管理が可能となる。
【００７６】
［９．ＷＡＮ側ユーザからのＳＯＨＯ環境内サービスへのアクセス］
ネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）のＳＡＬｄは、サービスアクセス機器リストに基づくＷＡＮ側クライアントからの、提供サービスの選択を受けて、ファイアフォールを設定後、そのサービスに対する外部ポート番号をユーザに伝達する。ユーザはその外部ポート番号で、例えば、
ｈｔｔｐ：／／４３．１１．１３５．８７：８０００
などのＵＲＬで、その指定したサービスにアクセス可能になる。
上記ＵＲＬの［４３．１１．１３５．８７］は、ＳＯＨＯルータのグローバルＩＰアドレスであり、［８０００］は、サービスに対応する外部ポート番号である。
【００７７】
ＳＯＨＯルータは、上記ＵＲＬを前述のＮＡＴ変換テーブル（図７）に基づいて、サービスを提供するＩＰ端末のプライベートアドレスと、内部ポート番号に変換して、接続を実行する。
【００７８】
［１０．セッションの開始］
ＷＡＮ側クライアントがネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）のＳＡＬｄから教えられたＵＲＬなどを使用して、ＳＯＨＯ環境内サービスとセッションを確立し、通信を開始する。
【００７９】
図１３に、ネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）のＳＡＬｄによるＬＡＮ側の内部端末のサービス登録処理、ＷＡＮ側端末からのアクセス要求に対する処理をまとめたシーケンス図を示す。
【００８０】
図１３の上段（ａ）は、ネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）のＳＡＬｄの管理ＩＰ端末のサービス登録処理である。
【００８１】
まず、登録要求がＩＰ端末のＳＡＬｄｃからネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）のＳＡＬｄに送信される登録メッセージは、図６に示す通りである。ＳＡＬｄは、登録メッセージに基づいて、管理データ（図８）を生成し、ＮＡＴ変換テーブル（図７）を生成し、登録完了メッセージをＩＰ端末のＳＡＬｄｃに送信する。その後は、定期的にサービスの起動状況をＫＥＥＰ ＡＬＩＶＥの送信、ＩＰ端末からのＡＣＫ受信により監視し、ＡＣＫがなかった場合には、管理データから登録サービスを削除する。ＩＰ端

末のＳＡＬｄｃは、サービス提供可否の状態情報としてサービス提供可である場合にのみＡＣＫをＳＡＬｄに対して出力する。

【００８２】

図１３の（ｂ）は、ＷＡＮ側クライアントからのサービス・リクエストに対する処理を示している。ＷＡＮ側クライアントは、ネットワーク接続機器（ｅｘ．ルータ、ゲートウェイ）に対してサービスアクセス機器リスト（図９）の提供を要求すると、ＳＡＬｄは、要求クライアントに対してユーザＩＤ，パスワードの入力を求め、入力されたユーザＩＤ．パスワードによる認証処理を実行する。なお、認証の形態は、セキュリティレベルに応じてその他の認証方法、例えば公開鍵暗号方式、共通鍵暗号方式などを適用してもよい。

【００８３】

認証が成功すると、ＳＡＬｄは、要求クライアントに対してサービスアクセス機器リスト（図９）を提供する。クライアントは、リストに基づいてサービスを選択し、ＳＡＬｄは、クライアントのＩＰアドレス（送信元アドレス）と選択サービスに従って、ファイアウォール（図１２参照）を設定する。

【００８４】

その後、ＳＡＬｄは、要求クライアントに対して、要求のあったサービスに対するアクセスに必要な情報としてＵＲＬ、具体的には、ネットワーク接続機器ｅｘ．ルータ、ゲートウェイ）のグローバルアドレス、サービスに対応する外部ポート番号を設定したＵＲＬを提供する。

【００８５】

ＷＡＮ側クライアントは、提示されたＵＲＬに基づいて、ＬＡＮ側ＩＰ端末のサービスに対するアクセスを実行する。なお、この際ＮＡＴにおいて、図７に示すＮＡＴ変換テーブルを用いたアドレス変換として、プライベートＩＰアドレスと内部ポート番号へ変換が実行される。

【００８６】

このように、本発明のシステムによれば、ルータ、ゲートウェイなど、通信中継装置であるネットワーク接続機器の管理下の端末のサービスの状態を定期的に監視して、サービスが不可能になった場合、あるいは新たなサービスが追加された場合などにその状態を更新し、常に最新の状態に保持したデータを保有する構成とするとともに、インターネット等の外部ネットワークからのアクセスを要求するクライアントに対してアクセス可能なサービスの情報をサービスアクセス機器リストによって提示し、選択したサービスに対して、ネットワーク接続機器がアドレス変換を行なって接続する構成としたので、ＷＡＮ側からＬＡＮ側へ、特定のサービスを指定したアクセスが可能となる。

【００８７】

なお、以上の構成は、ＩＰｖ４アドレス環境固有というものではなく、ＩＰｖ６環境に移行することなったとしても、ＳＯＨＯのＬＡＮ内部のネットワーク環境を外部に公開したくないという要求は同じであり、その場合、ＬＡＮ内部をＩＰｖ６リンクローカルアドレスで管理することになり、外部と直接インターネット接続を行わない構成となり、ＬＡＮ内部のサービス情報をＷＡＮ側のアクセス権限のあるユーザに見せる処理構成としては、上述した本発明の構成が適用可能である。

【００８８】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【発明の効果】

以上説明してきたように、本発明の通信中継装置、通信中継方法、通信端末装置、並びにプログラム記憶媒体によれば、ルータ、ゲートウェイなど、ネットワーク接続機器の管理下の端末のサービスの状態を定期的に監視して、提供可能なサービスを端末毎に管理し、

提供可能なサービスリストをインターネット等の外部ネットワークからのアクセスを要求するクライアントに対してリストによって提示し、クライアントの選択したサービスに対して、ネットワーク接続機器がアドレス変換を行なって接続する構成としたので、ＷＡＮ側からＬＡＮ側へ、特定のサービスを指定したアクセスが可能となる。

【００８９】

また、本発明の構成によれば、通信端末装置のサービスが不可能になった場合、あるいは新たなサービスが追加された場合などにその状態を更新し、常に最新の状態に保持したデータを保有する構成としたので、動的なＩＰ端末サービス管理が実行可能となる。

【００９０】

また、本発明の構成によれば、ＷＡＮ側からのクライアントに対しては、認証を行なって認証が成立した場合にのみサービスアクセス機器リストを提示する構成としたので、不正なユーザによる内部環境の漏洩が防止される。

【００９１】

【図面の簡単な説明】

【図１】従来のＮＡＴを用いたプライベートアドレスとグローバルアドレス間でのデータ通信態様を説明する図である。

【図２】従来のＩＰマスカレードを用いたプライベートアドレスとグローバルアドレス間でのデータ通信態様を説明する図である。

【図３】本発明のシステム構成の例を示す図である。

【図４】本発明のシステム構成としての階層構成の例を示す図である。

【図５】本発明のサービスアクセス機器リスト管理デーモン（ＳＡＬｄ）とサービス監視デーモン（ＳＡＬｄｃ）の実行するサービス登録処理を説明する図である。

【図６】本発明のサービスアクセス機器リスト管理デーモン（ＳＡＬｄ）とサービス監視デーモン（ＳＡＬｄｃ）の実行するサービス登録処理における登録メッセージ例を示す図である。

【図７】本発明の構成におけるネットワーク接続機器の有するＮＡＴ変換テーブルの例を示す図である。

【図８】本発明の構成におけるネットワーク接続機器の有する端末管理データの例を示す図である。

【図９】本発明の構成におけるネットワーク接続機器が提供するサービスアクセス機器リストの例を示す図である。

【図１０】本発明の構成におけるネットワーク接続機器の実行するサービス登録処理、更新処理を説明するフロー図である。

【図１１】本発明の構成におけるネットワーク接続機器の実行するサービス登録処理、更新処理におけるタイマー処理を説明するフロー図である。

【図１２】本発明の構成におけるネットワーク接続機器の生成するファイアウォールの例を示す図である。

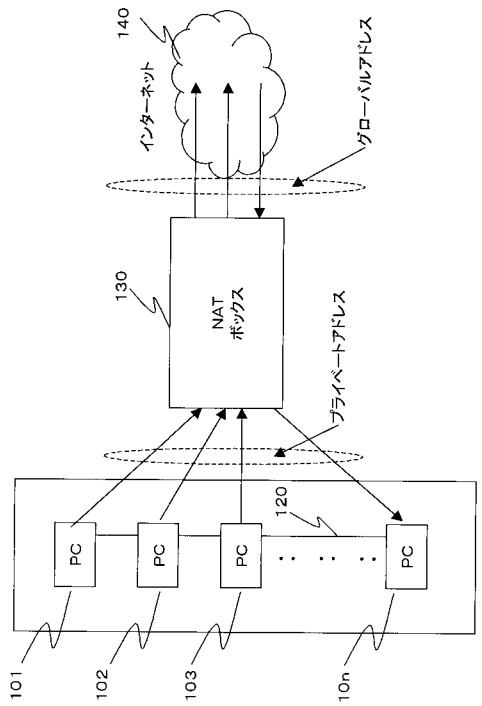
【図１３】本発明の構成におけるネットワーク接続機器の実行する処理シーケンスを示す図である。

【符号の説明】

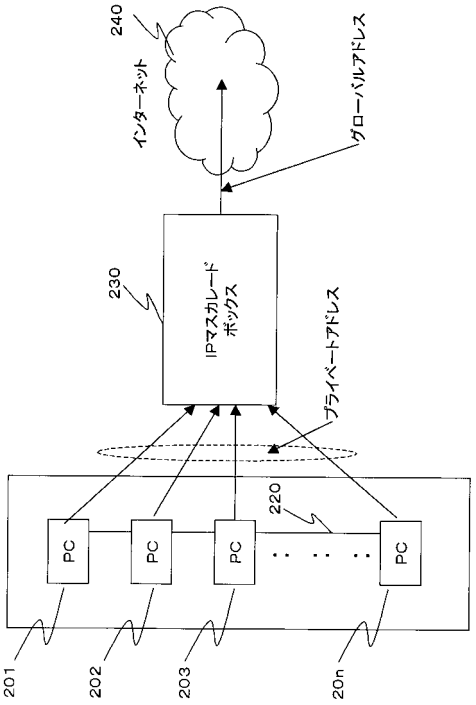
１０１～１０ｎ　通信端末
１２０　ＬＡＮ
１３０　ＮＡＴボックス
１４０　インターネット
２０１～２０ｎ　通信端末
２２０　ＬＡＮ
２３０　ＩＰマスカレードボックス
２４０　インターネット
３１０　ＳＯＨＯルータ
３１１　ＩＰ端末１

３１２　ＩＰ端末２
３２０　ＳＯＨＯルータ
３２１　ＨＴＴＰサーバ
３２２　ＦＴＰサーバ
３２３　ＲＴＳＰサーバ
４０１　ＳＯＨＯルータ
４０２　ＰＣ１
４０３　アプリケーションゲートウェイＰＣ２
４０４　カメラ
４０５　デッキ
４０６　ＵＳＢ機器

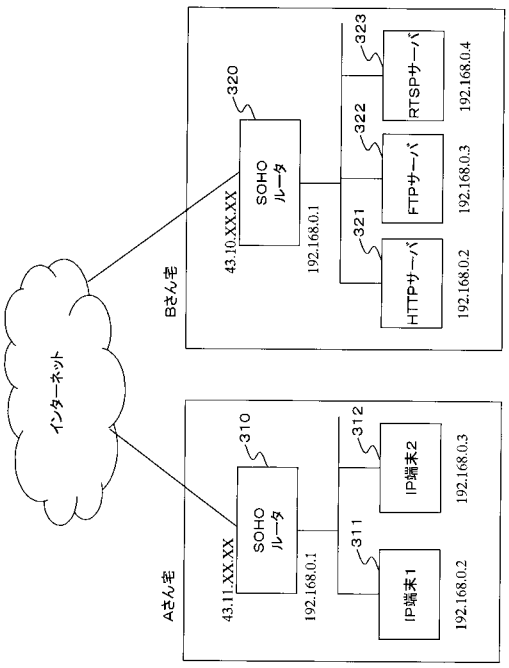
【図１】



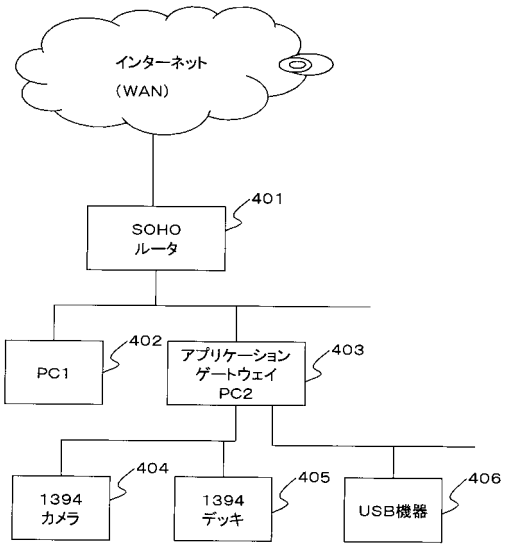
【図２】



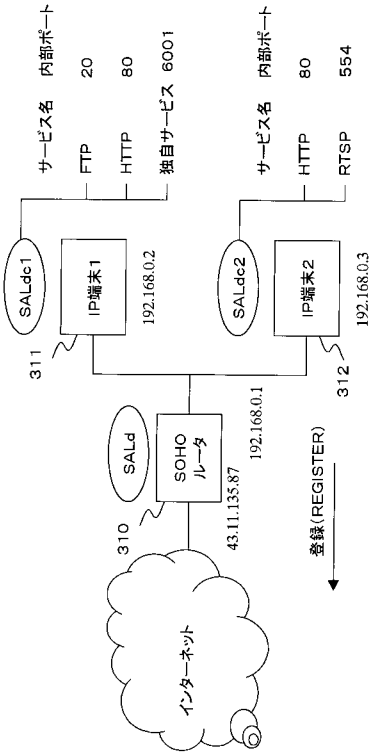
【図３】



【図４】



【図５】



【図６】

登録メッセージ

プライベートIPアドレス	端末名	端末属性	サービス名	サービス属性	内部ポート番号
192.168.0.2	IP端末1	PC	FTP	データ転送	20
192.168.0.2	IP端末1	PC	HTTP	インターネット	80
192.168.0.2	IP端末1	PC	独自サービス	映像、音楽	6001

【図７】

NAT変換テーブル

変換前 宛先IPアドレス	変換前 宛先ポート番号 (外部ポート番号)	変換後 宛先IPアドレス	変換後 宛先ポート番号 (内部ポート番号)
43.11.135.87	8000	192.168.0.2	20
43.11.135.87	8001	192.168.0.2	80
43.11.135.87	8002	192.168.0.2	6001
43.11.135.87	8003	192.168.0.3	80
43.11.135.87	8004	192.168.0.3	554

【図８】

端末管理データ

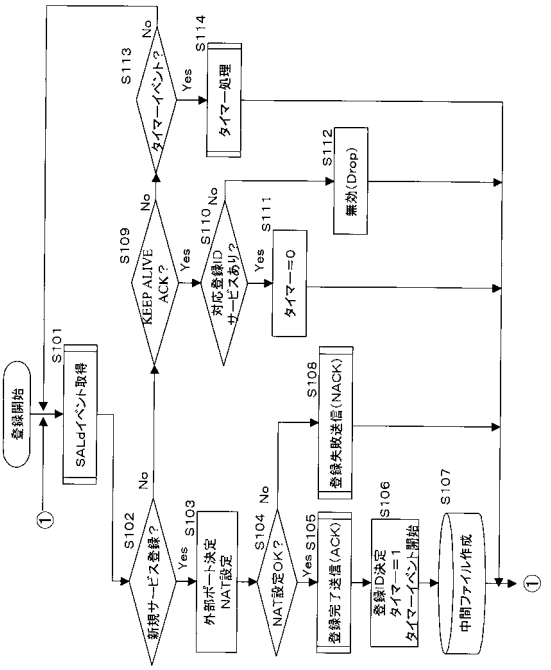
プライベート IPアドレス	端末名	端末属性	サービス名	サービス属性	外部ポート番号	内部ポート番号
192.168.0.2	IP端末1	PC	FTP	データ転送	8000	20
192.168.0.2	IP端末1	PC	HTTP	インターネット	8001	80
192.168.0.2	IP端末1	PC	独自サービス	映像、音楽	8002	6001
192.168.0.3	IP端末2	携帯端末	HTTP	インターネット	8003	80
192.168.0.3	IP端末2	携帯端末	RTSP	映像配信	8004	554

【図９】

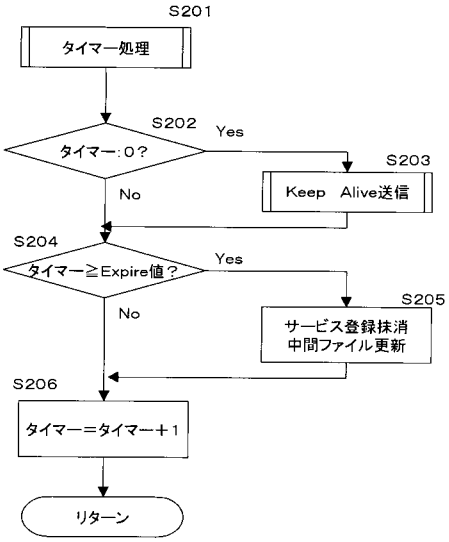
サービスアクセ機器リスト

端末名	端末属性	サービス名	サービス属性
IP端末1	PC	FTP	データ転送
IP端末1	PC	HTTP	インターネット
IP端末1	PC	独自サービス	映像、音楽
IP端末2	携帯端末	HTTP	インターネット
IP端末2	携帯端末	RTSP	映像配信

【図１０】



【図１１】

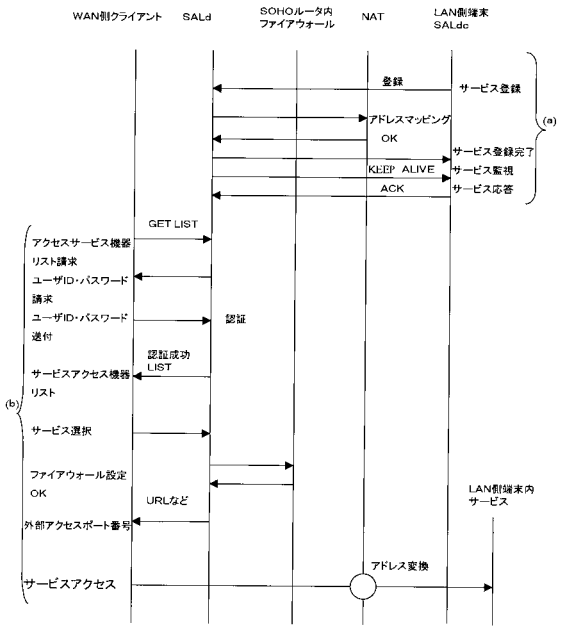


【図１２】

ファイアウォール

送信元IPアドレス	宛先IPアドレス	宛先ポート番号	動作
43.10.133.89	43.11.135.87	8000	通過許可
—	43.11.135.87	—	通過禁止

【図１３】



フロントページの続き

(56)参考文献 特開２０００－１３８６９６（ＪＰ，Ａ）
特開平１１－１２２３０１（ＪＰ，Ａ）
特開２００２－１４１９５４（ＪＰ，Ａ）
斉藤、高畠、橋本、岡本，デジタル情報家電の接続を考慮した家庭ネットワークアーキテクチャ Homenetwork Architecture Considering Digital Home Appliances，電子情報通信学会技術研究報告 Ｖｏｌ．９７ Ｎｏ．３６８ IEICE Technical Report，日本，社団法人電子情報通信学会 The Institute of Electronics,Information and Communication Engineers，１９９７年１１月，第97巻
久保 元治 MOTOHARU KUBO，技術解説，日経コンピュータ NIKKEI COMPUTER，日本，日経ＢＰ社

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 12/66
G06F 13/00
H04L 29/08