(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4950589号
(P4950589)
(45)発行日　平成24年6月13日(2012.6.13)　(24)登録日　平成24年3月16日(2012.3.16)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 353C
G06F 13/00 351Z

請求項の数 5　(全 14 頁)

(21)出願番号　特願2006-214001(P2006-214001)
(22)出願日　平成18年8月7日(2006.8.7)
(65)公開番号　特開2008-40772(P2008-40772A)
(43)公開日　平成20年2月21日(2008.2.21)
審査請求日　平成21年7月10日(2009.7.10)

(73)特許権者　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(74)代理人　100092820
弁理士　伊丹　勝
(74)代理人　100106389
弁理士　田村　和彦
(72)発明者　薩山　佳輝
東京都港区芝浦一丁目１番１号　株式会社東芝内

審査官　▲高▼都　広大

最終頁に続く

(54)【発明の名称】接続管理システム、接続管理方法、および管理サーバ

(57)【特許請求の範囲】
【請求項１】
外部ネットワークに接続されたクライアント端末と、前記クライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する接続管理システムであって、
前記外部ネットワークに接続された前記クライアント端末からのデータと、前記内部ネットワークセグメントに設置されたホストＰＣからのデータとをセッション毎に一意に定められたセッションＩＤを用いて中継するリバースプロキシサーバと、
前記外部ネットワークに接続された前記クライアント端末から前記リバースプロキシサーバを介して受信した前記ホストＰＣへの接続要求に対して、前記ホストＰＣのホストＰＣ名と前記ホストＰＣが提供可能なコンテンツとを含むホストＰＣデータに基づいて前記ホストＰＣへの接続の可否を決定し、接続可の場合には前記セッションＩＤを生成して前記リバースプロキシサーバおよび前記ホストＰＣに前記セッションＩＤを通知するとともに接続開始要求を行う管理サーバとを備え、
前記ホストＰＣは、前記管理サーバからの接続開始要求を受けたあと、前記管理サーバから受信した前記セッションＩＤを付加してデータを送信し、
前記リバースプロキシサーバは、前記ホストＰＣからの前記セッションＩＤが付加されたデータの受信に応じて当該データを前記クライアント端末に送信し、前記クライアント端末からのデータの受信に応じて当該データに前記セッションＩＤを付加して前記ホストＰＣに送信し

前記ホストＰＣデータは、同一のコンテンツを提供するホストＰＣが前記内部ネットワークセグメントに複数設置されている場合における当該ホストＰＣ群のグループ名、接続可能なクライアント端末の最大数、クライアント端末との現在の接続数、現在の負荷状況、および最大許容負荷を含み、
各ホストＰＣは、自己のホストＰＣデータを定期的に更新し、
前記管理サーバは、前記外部ネットワークに接続された前記クライアント端末から前記リバースプロキシサーバを介して受信した接続要求が前記グループ名を指定した接続要求であった場合には、当該接続要求に対して、前記ホストＰＣデータに基づいて、接続の可能なホストＰＣが複数存在した場合には、接続可能なクライアント端末の最大数と現在の接続数との差が最大のホストＰＣ、あるいは最大許容負荷と現在の負荷状況との差が最大のホストＰＣへの接続を許可する
ことを特徴とする接続管理システム。
【請求項２】
前記ホストＰＣは、前記管理サーバからの接続開始要求に応じて、前記管理サーバから受信した前記セッションＩＤを前記リバースプロキシサーバに送信することで当該リバースプロキシサーバとの接続を開始するとともに、前記ホストＰＣに各種の処理を実行させるための既存サーバプログラムの待ち受けポート番号に向けた接続を開始し、前記リバースプロキシサーバとの接続を開始したあと、前記セッションＩＤを付加してデータを送信する
請求項１に記載の接続管理システム。
【請求項３】
前記ホストＰＣは、
起動時に、問い合わせ用のブロードキャストパケットを送信し、
前記ブロードキャストパケットを送信したあと一定期間が経過するまでに管理サーバとして機能している他のホストＰＣからの応答がなかった場合、前記リバースプロキシサーバに対して管理サーバとしての接続依頼を行う
請求項１又は請求項２に記載の接続管理システム。
【請求項４】
外部ネットワークに接続されたクライアント端末と、前記クライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する接続管理方法であって、
前記外部ネットワークに接続された前記クライアント端末から、該クライアント端末からのデータと前記ホストＰＣからのデータとを中継するリバースプロキシサーバを介して前記ホストＰＣへの接続要求を受信し、
受信した接続要求に対して、前記ホストＰＣのホストＰＣ名と前記ホストＰＣが提供可能なコンテンツとを含み、同一のコンテンツを提供するホストＰＣが前記内部ネットワークセグメントに複数設置されている場合における当該ホストＰＣ群のグループ名、接続可能なクライアント端末の最大数、クライアント端末との現在の接続数、現在の負荷状況、および最大許容負荷を含むホストＰＣデータに基づいて前記ホストＰＣへの接続の可否を決定し、
接続可の場合には前記セッションＩＤを生成して前記リバースプロキシサーバおよび前記ホストＰＣに前記セッションＩＤを通知するとともに接続開始要求を行い、
前記ホストＰＣにおいて、前記接続開始要求を受けたあと、受信した前記セッションＩＤを付加してデータを送信させ、
前記リバースプロキシサーバにおいて、前記ホストＰＣからの前記セッションＩＤが付加されたデータの受信に応じて当該データを前記クライアント端末に送信させ、前記クライアント端末からのデータの受信に応じて当該データに前記セッションＩＤを付加して前記ホストＰＣに送信し、
各ホストＰＣにおいて、自己のホストＰＣデータを定期的に更新させ、
前記外部ネットワークに接続された前記クライアント端末から前記リバースプロキシサ

ーバを介して受信した接続要求が前記グループ名を指定した接続要求であった場合には、当該接続要求に対して、前記ホストＰＣデータに基づいて、接続の可能なホストＰＣが複数存在した場合には、接続可能なクライアント端末の最大数と現在の接続数との差が最大のホストＰＣ、あるいは最大許容負荷と現在の負荷状況との差が最大のホストＰＣへの接続を許可する
ことを特徴とする接続管理方法。
【請求項５】
外部ネットワークに接続されたクライアント端末と、前記クライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する管理サーバであって、
前記ホストＰＣのホストＰＣ名と前記ホストＰＣが提供可能なコンテンツとを含むホストＰＣデータを記憶する記憶手段と、
前記外部ネットワークに接続された前記クライアント端末からリバースプロキシサーバを介して受信した前記ホストＰＣへの接続要求に対して、前記ホストＰＣデータに基づいて前記ホストＰＣへの接続の可否を決定し、前記外部ネットワークに接続された前記クライアント端末から前記リバースプロキシサーバを介して受信した前記ホストPCへの接続要求に対して、前記ホストＰＣデータに基づいて、接続の可能なホストＰＣが複数存在した場合には、接続可能なクライアント端末の最大数と現在の接続数との差が最大のホストＰＣ、あるいは最大許容負荷と現在の負荷状況との差が最大のホストＰＣへの接続を許可する
接続決定手段と、
該接続決定手段が接続可と決定した場合にセッション毎に一意に定められるセッションＩＤを生成し、前記クライアント端末からのデータと前記ホストＰＣからのデータとをセッションＩＤを用いて中継する前記リバースプロキシサーバおよび前記ホストＰＣに対して前記セッションＩＤを通知する通知手段と、
前記ホストＰＣに対して、前記リバースプロキシサーバとの間で前記セッションＩＤを付加してデータ通信を行わせるための接続開始要求を行う開始要求手段と
を備えることを特徴とする管理サーバ。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部ネットワークに接続されたクライアント端末と、そのクライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する接続管理システム、接続管理方法、および管理サーバに関するものである。
【背景技術】
【０００２】
従来から、外部ネットワーク上のクライアントからイントラネット内のホストＰＣにアクセスするためのシステムがある。このシステムにおいては、ホストＰＣと外部ネットワーク上のクライアントとの通信を行う際に、二者間にファイアウォールが存在していても通信パケットが通過できるようにするため、その通信プロトコルをＨＴＴＰ（HyperText Transfer Protocol）などのファイアウォールの通過を許可されたプロトコルに変換して送信し、イントラネット内のプロキシサーバで再度ホストＰＣ向けへの通信プロトコルに変換し直すこととしている（特許文献１）。
【０００３】
ファイアウォールの内側にあるイントラネット内のサーバへの接続を外部ネットワーク上のクライアントから行うことができるようにするための技術は、従来からいくつか提案されている。例えば、クライアントプログラムとサーバプログラムとの通信を中継する中継サーバを設け、その中継サーバおよびクライアントにデータの送信先を示す経路情報を保持するためのテーブルを持たせておき、通信を開始するときに、その経路情報をクライ

アントから順にたどっていくことによってサーバまでの経路を特定し、クライアントからサーバまでの通信を確立することとしたものがある（特許文献２）。

【０００４】

【特許文献１】特開２００４－５４２７号公報

【特許文献２】特開２００１－２５１３６７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

上述した特許文献１に記載された発明では、内部ネットワークにクライアントからのパケットを入力することは可能とされているが、その後のホストＰＣまでの接続管理処理については考慮されていない。

【０００６】

また、上述した特許文献２に記載された発明では、サーバプログラムの待ち受けポートへ向かう通信パケットおよびその応答パケットについては各ファイアウォールにて事前に通過許可を受けていなくてはならない。すると、サーバにて提供するサービスが増えるごとに、各ファイアウォールにて通過許可のための処理を行う必要のある待ち受けポートが増えるので、その分ネットワーク全体のセキュリティが低下してしまうことにつながる。すなわち、ファイアウォールの設定にて通過許可するパケットを必要最小限度に抑えながら、クライアント／サーバ間の通信を確立する手法が必要であるが、そのような手法についてまで考慮されてはいない。

【０００７】

Ｐ２Ｐ（Peer to Peer）型の接続方法を用いたＳｋｙｐｅ（スカイプ：Ｐ２Ｐ技術を応用した音声通話ソフトウェア）の場合、呼び出し先のＰＣがＮＡＴ（Network Address Translation）ルータの内側にある場合にも通話が開始できるようにするため、Ｓｋｙｐｅをインストールしたクライアントの中からスーパーノードと呼ばれるサーバを選定している。スーパーノードへの制御用接続を、呼び出し先のＰＣ、呼び出し元ＰＣとも先に作成しておき、呼び出しが発生した際には制御用接続を用いてＮＡＴルータの内側にいる呼び出し先ＰＣに呼処理開始を通知してＮＡＴルータの内側にいるホスト側から通信を開始させることで、ＮＡＴルータを通過させるようにしている。しかし、Ｐ２Ｐ通信で唯一のサービスを提供することが前提となっているため、ホストＰＣが複数のユーザに同一のサービスを提供できる場合もしくは複数のホストＰＣが同一のサービスをユーザに対して提供できる場合に、サービスを振り分けるなどの機能は考慮されていない。また、サービス提供可能なホストＰＣの電源が一時的に落とされている場合に、それを自動的に立ち上げてサービス提供を開始させる機能についても考慮されていない。

【０００８】

本発明は、かかる問題点に鑑みてなされたもので、ホストＰＣがＮＡＴルータやファイアウォールで保護されているネットワークセグメント内部に設置されているホストＰＣと外部ネットワークに接続されているクライアント端末との接続を、外部ネットワーク側で接続管理することなく容易に確立できるようにすることを目的とする。

【課題を解決するための手段】

【０００９】

本発明に係る接続管理システムは、外部ネットワークに接続されたクライアント端末と、前記クライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する接続管理システムであって、前記外部ネットワークに接続された前記クライアント端末からのデータと、前記内部ネットワークセグメントに設置されたホストＰＣからのデータとをセッション毎に一意に定められたセッションＩＤを用いて中継するリバースプロキシサーバと、前記外部ネットワークに接続された前記クライアント端末から前記リバースプロキシサーバを介して受信した前記ホストＰＣへの接続要求に対して、前記ホストＰＣのホストＰＣ名と前記ホストＰＣが提供可能なコンテンツとを含むホストＰＣデータに基づいて前記ホストＰＣへの接続の可否を決定し、接続

可の場合には前記セッションＩＤを生成して前記リバースプロキシサーバおよび前記ホストＰＣに前記セッションＩＤを通知するとともに接続開始要求を行う管理サーバとを備え、前記ホストＰＣは、前記管理サーバからの接続開始要求を受けたあと、前記管理サーバから受信した前記セッションＩＤを付加してデータを送信し、前記リバースプロキシサーバは、前記ホストＰＣからの前記セッションＩＤが付加されたデータの受信に応じて当該データを前記クライアント端末に送信し、前記クライアント端末からのデータの受信に応じて当該データに前記セッションＩＤを付加して前記ホストＰＣに送信することを特徴とする。本発明に係る接続管理システムによれば、ホストＰＣがＮＡＴルータやファイアウォールで保護されているネットワークセグメント内部に設置されているホストＰＣと外部ネットワークに接続されているクライアント端末との接続を、外部ネットワーク側で接続管理することなく容易に確立することができるようになる。

【００１０】

本発明に係る接続管理方法は、外部ネットワークに接続されたクライアント端末と、前記クライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する接続管理方法であって、前記外部ネットワークに接続された前記クライアント端末から、該クライアント端末からのデータと前記ホストＰＣからのデータとを中継するリバースプロキシサーバを介して前記ホストＰＣへの接続要求を受信し、受信した接続要求に対して、前記ホストＰＣのホストＰＣ名と前記ホストＰＣが提供可能なコンテンツとを含むホストＰＣデータに基づいて前記ホストＰＣへの接続の可否を決定し、接続可の場合には前記セッションＩＤを生成して前記リバースプロキシサーバおよび前記ホストＰＣに前記セッションＩＤを通知するとともに接続開始要求を行い、前記ホストＰＣは、前記接続開始要求を受けたあと、受信した前記セッションＩＤを付加してデータを送信し、前記リバースプロキシサーバは、前記ホストＰＣからの前記セッションＩＤが付加されたデータの受信に応じて当該データを前記クライアント端末に送信し、前記クライアント端末からのデータの受信に応じて当該データに前記セッションＩＤを付加して前記ホストＰＣに送信することを特徴とする。本発明に係る無線通信方法によれば、ホストＰＣがＮＡＴルータやファイアウォールで保護されているネットワークセグメント内部に設置されているホストＰＣと外部ネットワークに接続されているクライアント端末との接続を、外部ネットワーク側で接続管理することなく容易に確立することができるようになる。

【００１１】

本発明に係る管理サーバは、外部ネットワークに接続されたクライアント端末と、前記クライアント端末に対してコンテンツを提供する内部ネットワークセグメントに設置されたホストＰＣとの接続を管理する管理サーバであって、前記ホストＰＣのホストＰＣ名と前記ホストＰＣが提供可能なコンテンツとを含むホストＰＣデータを記憶する記憶手段と、前記外部ネットワークに接続された前記クライアント端末からリバースプロキシサーバを介して受信した前記ホストＰＣへの接続要求に対して、前記ホストＰＣデータに基づいて前記ホストＰＣへの接続の可否を決定する接続決定手段と、該接続決定手段が接続可と決定した場合にセッション毎に一意に定められるセッションＩＤを生成し、前記クライアント端末からのデータと前記ホストＰＣからのデータとをセッションＩＤを用いて中継する前記リバースプロキシサーバおよび前記ホストＰＣに対して前記セッションＩＤを通知する通知手段と、前記ホストＰＣに対して、前記リバースプロキシサーバとの間で前記セッションＩＤを付加してデータ通信を行わせるための接続開始要求を行う開始要求手段とを備えることを特徴とする。

【発明の効果】

【００１２】

本発明によれば、ホストＰＣがＮＡＴルータやファイアウォールで保護されているネットワークセグメント内部に設置されているホストＰＣと外部ネットワークに接続されているクライアント端末との接続を、外部ネットワーク側で接続管理することなく容易に確立することができる接続管理システム、および接続管理方法、および管理サーバを提供する

ことができる。
【発明を実施するための最良の形態】
【００１３】
以下、図面に基づいて本発明の実施形態に係るネットワーク接続管理システムについて説明する。
【００１４】
［実施形態１］
図１は、ネットワーク接続管理システムの構成の例を示すブロック図である。図１に示すように、ネットワーク接続管理システムは、クライアント端末１０と、ファイアウォール２０と、リバースプロキシサーバ３０と、ＮＡＴルータ４０と、内部ネットワークセグメント５０とを含む。
【００１５】
内部ネットワークセグメント５０内には、管理サーバ５１と、複数のホストＰＣ５２，５３，５４とが設けられている。管理サーバ５１と、複数のホストＰＣ５２，５３，５４とは、それぞれ、ＬＡＮなどの通信ネットワークによって接続されている。管理サーバ５１は、ホストＰＣ５２，５３，５４からリバースプロキシサーバ３０までの接続を確立するためのサーバ装置である。なお、図１ではホストＰＣ５２，５３，５４を３台としているが、ホストＰＣの台数は何台であってもよい。
【００１６】
本例のネットワーク接続管理システムでは、リバースプロキシサーバ３０が、インターネットなどの外部通信ネットワーク６０に接続されたクライアント端末１０からのアクセスを一旦受け付ける。なお、ここではクライアント端末が１台であるものとしているが、クライアント端末は何台接続されていてもよい。また、クライアント端末１０から接続したいホストＰＣ５２，５３，５４は、内部ネットワークセグメント５０内に設置されている。また、通信ネットワークの独立性を保つために、リバースプロキシサーバ３０と内部ネットワークセグメント５０との間にはＮＡＴルータ４０が設置されている。
【００１７】
このため、リバースプロキシサーバ３０からは、ホストＰＣ５２，５３，５４に直接アクセスすることはできない。内部ネットワークセグメント５０内に設けられた管理サーバ５１が、ホストＰＣ５２，５３，５４に関わるデータ（ホストＰＣデータ）を保持・管理し、リバースプロキシサーバ３０からの接続要求を処理する。
【００１８】
次に、リバースプロキシサーバ３０、管理サーバ５１、およびホストＰＣ５２，５３，５４の内部機能について説明する。ここでは、ホストＰＣ５２，５３，５４のうちホストＰＣ５２について説明するが、他のホストＰＣ５３，５４も同様である。
【００１９】
図２は、リバースプロキシサーバ３０、管理サーバ５１、およびホストＰＣ５２の内部機能を説明するためのブロック図である。
【００２０】
図２に示すように、リバースプロキシサーバ３０は、プロトコル変換部３１と、コマンド通信部３２と、サービス通信部３３とを含む。また、管理サーバ５１は、コマンド通信部５１１と、サービス接続管理部５１２と、ホストＰＣデータ受信部５１３と、ホストＰＣデータＤＢ５１４とを含む。なお、ホストＰＣデータＤＢ５１４は、管理サーバ５１の内部に設けられていても外部に設けられていてもよい。さらに、ホストＰＣ５２は、管理サーバ間通信部５２１と、ホストＰＣデータ取得部５２２と、サービス通信部５２３と、サービス内容ＤＢ５２４とを含む。なお、サービス内容ＤＢ５２４は、ホストＰＣ５２の内部に設けられていても外部に設けられていてもよい。
【００２１】
本例のネットワーク接続管理システムのように、外部通信ネットワーク６０と内部ネットワークセグメント５０との間にファイアウォール２０が設置され、外部ネットワーク６

０と内部ネットワークセグメント５０との間にアクセス制限が設けられているものが、一般的なネットワーク構成である。このような一般的なネットワーク構成である場合にも、クライアント端末１０と内部ネットワークセグメント５０内にあるホストＰＣ５２，５３，５４のいずれかとの間で接続が可能になるように、クライアント端末１０およびリバースプロキシサーバ３０は、ファイアウォールを通過できるプロトコルに変換するためのプロトコル変換部１１を持つ。プロトコル変換部１１は、本例では、クライアント端末１０からのメッセージをその種類にしたがって接続処理に関するコマンドを扱うコマンド通信部３２もしくはホストＰＣ５２，５３，５４との接続そのものに利用されるデータを扱うサービス通信部３３のいずれかに振り分ける。

【００２２】

管理サーバ５１は、ホストＰＣデータ受信部５１３で同一ネットワークセグメント内に設置されたホストＰＣ５２，５３，５４から接続管理に必要なホストＰＣデータを定期的に受信し、ホストＰＣデータＤＢ５１４内のホストＰＣデータを更新する。なお、ホストＰＣ５２，５３，５４がホストＰＣデータＤＢ５１４内の自己のホストＰＣデータを定期的に更新し、管理サーバ５１のホストＰＣデータ受信部５１３が、ホストＰＣデータＤＢ５１４内のホストＰＣデータを定期的に確認するようにしてもよい。

【００２３】

図３は、ホストＰＣデータＤＢ５１４に格納されているホストＰＣデータの例を示す説明図である。図３に示すように、ホストＰＣデータは、ホストＰＣ名、ＭＡＣ（Media Access Control）アドレス、所属グループ名、提供可能なコンテンツなどのサービスを示す提供可能サービス名、接続可能なクライアント端末の最大数を示す接続最大数または発行可能なセッションＩＤの最大数を示すセッションＩＤ発行可能最大数、現在接続中のクライアント端末数、サービス可能ネットワークパケット量最大値、現ネットワークパケット量、などのホストＰＣに係る各種の情報を含む。ホストＰＣデータは、各ホストＰＣ毎に設定される。

【００２４】

ホストＰＣデータのうち、「現ネットワークパケット量」はホストＰＣ５２のサービス通信部５２３から取得し、残りのデータはホストＰＣデータ取得部５２２から設定値を取得する。「所属グループ名」は、複数のホストＰＣが同一のサービスをユーザに対して提供できる場合に使用されるＩＤ値である。受信したホストＰＣデータをホストＰＣデータＤＢ５１４に格納しておき、クライアント端末１０からリバースプロキシサーバ３０内のコマンド通信部３２を経て管理サーバ５１内のコマンド通信部５１１で受信した接続要求に対してホストＰＣ５２上のサービスへの接続を許可するかどうか、また複数のホストＰＣが同一のサービスをユーザに対して提供できる場合にどのホストＰＣに接続要求を送信するかを決める際のデータとする。

【００２５】

クライアント端末１０からの接続要求を処理するためには、リバースプロキシサーバ３０から管理サーバ５１までの接続を事前に確立させておく必要がある。管理サーバ５１のコマンド通信部５１１は、起動直後にリバースプロキシサーバ３０のコマンド通信部３２へ向けてＴＣＰ（Transmission Control Protocol）接続を開始する。管理サーバ５１側から接続を開始することで、リバースプロキシサーバ３０と管理サーバ５１の間にＮＡＴルータ４０が存在している場合でも容易に接続を開始することができる。負荷分散などの理由でリバースプロキシサーバ３０が複数存在する場合は、接続要求処理用の接続はそれぞれのリバースプロキシサーバに対して確立しておくようにすればよい。

【００２６】

次に、リバースプロキシサーバ３０がクライアント端末１０から接続要求を受けた場合の管理サーバ５１内部の処理について説明する。図４は、管理サーバ５１が実行する接続管理処理の例を示すフローチャートである。

【００２７】

接続管理処理において、管理サーバ５１は、クライアント端末１０からの接続要求をリ

バースプロキシサーバ３０を介して受信すると（ステップＳ１０１）、接続要求にて指定されたホストＰＣもしくは所属グループ名（複数のホストＰＣで同一のサービスを提供している場合）、および提供可能サービス名を用いてホストＰＣデータＤＢ５１４を検索し、接続要求に合致するホストＰＣを抽出する（ステップＳ１０２）。

【００２８】

クライアント端末１０からの「接続要求」には、ホストＰＣ名もしくは所属グループ名および提供を希望するコンテンツを示す提供希望サービス名が含まれているものとする。管理サーバ５１に接続したことのあるホストＰＣのホストＰＣデータはすべてホストＰＣデータＤＢ５１４に残っているので、管理サーバ５１は、ステップＳ１０２にて、接続要求に含まれるホストＰＣ名もしくは所属グループ名および提供を希望するサービス名をキーに検索を行う。

【００２９】

次に、管理サーバ５１は、検索したホストＰＣ全てについて、現接続数が提供可能サービス数未満であり、かつ、現ネットワークパケット量がサービス可能ネットワークパケット量最大値未満であるか否か確認する（ステップＳ１０３）。

【００３０】

ステップＳ１０３における２つの条件を満たすホストＰＣが存在していなければ（ステップＳ１０４のＮ）、管理サーバ５１は、接続要求を満たす現在サービス可能なホストＰＣが存在しないため、リバースプロキシサーバ３０に対して接続拒否応答を行う（ステップＳ１０５）。

【００３１】

ステップＳ１０３における２つの条件を満たすホストＰＣが存在していた場合（ステップＳ１０４のＹ）、管理サーバ５１は、ステップＳ１０３における２つの条件を満たすホストＰＣが複数存在していれば、現ネットワークパケット量が最小のホストＰＣを選出する（ステップＳ１０６）。なお、ステップＳ１０６では、単純に現ネットワークパケット量が最小のホストＰＣを選出することとしてもよいし、サービス可能ネットワークパケット量最大値と現ネットワークパケット量との差が最大のホストＰＣを選出することとしてもよい。また、ステップＳ１０６にて、接続最大数と現在接続中のクライアント端末数との差が最大のホストＰＣを選出することとしてもよい。

【００３２】

上記のようにして、ステップＳ１０３における２つの条件を満たすホストＰＣのうち１つを選出する。ここでは、ホストＰＣ５２が選出されたものとする。すると、管理サーバ５１は、今回接続するサービス用に一意のセッションＩＤを生成し、選出されたホストＰＣ５２のサービス通信部５２３およびリバースプロキシサーバ３０のサービス通信部３３に対してセッションＩＤを通知し（ステップＳ１０７）、ホストＰＣ５２のサービス通信部５２３が無応答でなければ（ステップＳ１０８）、ホストＰＣ５２側からリバースプロキシサーバ３０へ向けたサービス提供のための接続を開始させる（ステップＳ１０９）。

【００３３】

以後の通信パケットには、サービス自体のデータペイロードのほかにこのセッションＩＤを必ず付与するようにする。すなわち、ホストＰＣ５２は、管理サーバ５１からの接続開始要求を受けたあと、管理サーバ５１から受信したセッションＩＤを付加してデータを送信する。そして、リバースプロキシサーバ３０は、ホストＰＣ５２からのセッションＩＤが付加されたデータの受信に応じて当該データをクライアント端末１０に送信し、クライアント端末１０からのデータの受信に応じて当該データにセッションＩＤを付加してホストＰＣ５２に送信する。このようにして、データ通信が実行される。このとき、ホストＰＣ５２のサービス通信部５２３が無応答になった場合には（ステップＳ１０８）、管理サーバ５１は、ホストＰＣ５２の電源が一時的に切れていると判断をして、ホストＰＣデータ中のＭＡＣアドレスを使用して「Wake On LAN機能」を用いたマジックパケットを送信する（ステップＳ１１０）。その後、接続開始待ち状態となる（ステップＳ１１１）。

【００３４】

上述したように、本発明の第１実施形態によれば、クライアント端末１０側にはリバースプロキシサーバ３０から内側の内部ネットワークセグメント５０の構成やホストＰＣの通信負荷などの状態を見せずに、ホストＰＣが複数のユーザに同一のサービスを提供できる場合もしくは複数のホストＰＣが同一のサービスをユーザに対して提供できる場合にも、どのホストＰＣにどのサービスを要求するかをホストＰＣが定期的に送信するネットワーク負荷などのデータをもとに判断し、適切なホストＰＣとの間で接続を行うことができるようになる。

【００３５】

すなわち、上述したように、外部ネットワーク６０に接続されたクライアント端末１０からのデータと、内部ネットワークセグメント５０に設置されたホストＰＣ５２からのデータとをセッションＩＤを用いて中継するリバースプロキシサーバ３０と、外部ネットワーク６０に接続されたクライアント端末１０からリバースプロキシサーバ３０を介して受信したホストＰＣ５２への接続要求に対して、ホストＰＣ５２のホストＰＣ名とホストＰＣが提供可能なコンテンツとを含むホストＰＣデータに基づいてホストＰＣ５２への接続の可否を決定し、接続可の場合にはセッション毎に一意のセッションＩＤを生成してリバースプロキシサーバ３０およびホストＰＣ５２にセッションＩＤを通知するとともに接続開始要求を行う管理サーバ５１とを備え、ホストＰＣ５２は、管理サーバ５１からの接続開始要求を受けたあと、管理サーバ５１から受信したセッションＩＤを付加してデータを送信し、リバースプロキシサーバ３０は、ホストＰＣ５２からのセッションＩＤが付加されたデータの受信に応じて当該データをクライアント端末１０に送信し、クライアント端末１０からのデータの受信に応じて当該データにセッションＩＤを付加してホストＰＣ５２に送信することを特徴とするので、ホストＰＣ５２がＮＡＴルータ４０やファイアウォール２０で保護されている内部ネットワークセグメント５０に設置されているホストＰＣ５２と外部ネットワーク６０に接続されているクライアント端末１０との接続を、外部ネットワーク６０側で接続管理することなく容易に確立することができるようになる。

【００３６】

また、上述したように、ＮＡＴルータ４０やファイアウォール２０で守られている内部ネットワークセグメント５０にホストＰＣ５２がある場合にも、接続をホストＰＣ５２側から始めることができるため、ホストＰＣ５２のＩＰアドレスやポート番号、ファイアウォール２０の設定などを、接続要求を送信したリバースプロキシサーバ３０側が管理する必要なしに接続を確立することができる。

【００３７】

また、上述したように、ホストＰＣ５２の電源が一時的に切られているなどの不慮の事態が発生しても、管理サーバ５１内のホストＰＣデータを参照することで、そのホストＰＣ５２にマジックパケットを送信し、「Wake on LAN機能」によってホストＰＣ５２を起動しなおすことも可能である。

【００３８】

なお、上述した実施の形態では特に言及していなかったが、ホストＰＣ上で稼動する既存のサーバプログラムへの接続方法については、図５に示すようになる。

【００３９】

ホストＰＣ５２上で稼動する既存サーバプログラム５２４があるとする。通常、ファイアウォール２０の外側にあるクライアント（図５ではリバースプロキシサーバ３０が該当する）から既存サーバプログラム５２４へアクセスする場合には、既存サーバプログラム５２４の待ち受けポートＸへの接続をファイアウォール２０で許可する必要があるが、セキュリティを確保するためにファイアウォール２０の外側から内側へ向かう接続を許可したくない場合にはこの方法を用いることができない。

【００４０】

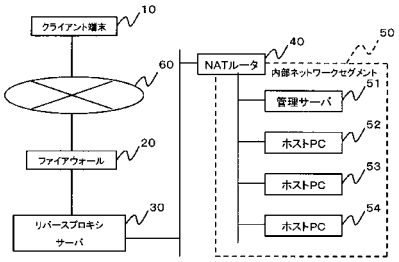
そこで、ホストＰＣ上で稼動させるサービス提供プログラム中のサービス通信部５２３を使用して、プロキシサーバ３０と既存サーバプログラム５２４との通信が成立できるようにする。

【００４１】
サービス通信部５２３は、上述したように、管理サーバからの接続要求を受け取り、リバースプロキシサーバ３０のサービス通信部３３への接続を開始する機能を有する。この機能によってサービス提供用の接続が確立されるが、このときサービス通信部５２３から既存サーバプログラム５２４の待ち受けポート番号Xに向けた接続も開始する。このようにすると、リバースプロキシサーバ３０側から既存サーバプログラム５２４へ直接接続することなくリバースプロキシサーバ３０と既存サーバプログラム５２４とのデータ通信を行うことができる。
【００４２】
すなわち、ホストＰＣ上で既存のサーバプログラムが稼動している場合に、リバースプロキシサーバ３０側から直接サーバプログラムの待ち受けポートに接続せずにサーバプログラムとリバースプロキシサーバ３０間の通信を確立することができる。これによって、内部ネットワークセグメント５０のセキュリティポリシーを大きく変更せずに、より安全な方法で既存のサーバプログラムとも通信を行うことができる。
【００４３】
［実施形態２］
上述した第１の実施形態では、内部ネットワークセグメント５０中に管理サーバ５１が必ず存在し、ホストＰＣ５２，５３，５４は管理サーバ５１との接続が確立できることが前提となっていた。現実には、常時管理サーバ５１を立ち上げておくことは負担が大きい。そこで、内部ネットワークセグメント５０中のホストＰＣ群のうち、どれか１つが管理サーバの機能を兼ねることができるようにする。このようにするためのホストＰＣ内のプログラム動作は、図６，図７に示すようになる。
【００４４】
図６，図７は、任意のホストＰＣを管理サーバとして機能させるために各ホストＰＣに実行させる処理の例を示すフローチャートである。図６は、起動時に実行される管理サーバ決定処理の例を示すフローチャートである。図７は、管理サーバ探索用ブロードキャストパケットの受信時の対応処理を示す探索用パケット応答処理の例を示すフローチャートである。本例では、図１に示す管理サーバ５１は存在せず、ホストＰＣ５２，５３，５４のいずれかが管理サーバ５１の機能を持つことになる。
【００４５】
管理サーバ決定処理において、ホストＰＣは、まず、起動時にブロードキャストパケットを送信し（ステップＳ２０１）、自己が属する内部ネットワークセグメント５０内に管理サーバが存在しているかどうかをチェックする（ステップＳ２０２）。
【００４６】
管理サーバ機能がいずれかのホストＰＣで動作している場合は、後述するように（ステップＳ３０３参照）、ブロードキャストパケットに対して応答が返ってくる。
【００４７】
応答があった場合には（ステップＳ２０２のＹ）、ホストＰＣは、応答のあった管理サーバ機能が動作しているホストＰＣを同定し、管理サーバとの接続をＴＣＰ通信にて確立する（ステップＳ２０３）。接続が確立した後は、ホストＰＣは、上述した第１の実施形態と同様に、ホストＰＣ名、ホストＰＣの所属するグループ名、提供可能なサービスの種類および最大提供サービス数、ホストＰＣの状態およびホストＰＣが送受信しているパケットの流量を計測したデータなどのホストＰＣデータを定期的に管理サーバとして機能しているホストＰＣに対して送信する（ステップＳ２０４）。
【００４８】
一方、ブロードキャストパケットに対して一定時間応答がなかった場合には（ステップＳ２０２のＮ）、ホストＰＣは、動作中の管理サーバがないと判断し、管理サーバとしての機能を自身で実行する。すなわち、ホストＰＣは、リバースプロキシサーバ３０への接続を試み（ステップＳ２０６）、その接続が許可された場合に（ステップＳ２０７）、管理サーバとして動作を開始する（ステップＳ２０８）。

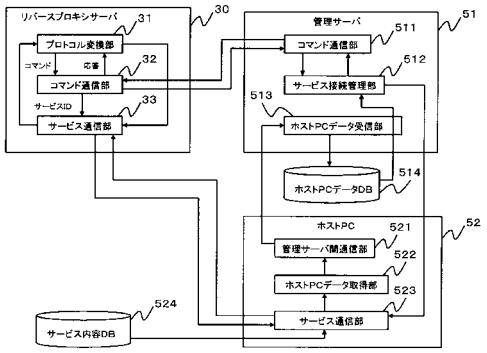
【００４９】
なお、管理サーバとの接続が切断されたことが検出できた場合には（ステップＳ２０５のＹ）、ホストＰＣは、ブロードキャストパケットを送信するところ（ステップＳ２０１）からやり直して再度管理サーバ機能を探索する。
【００５０】
上記の方法では、複数のホストＰＣが管理サーバ機能を実行しようとする可能性があるが、管理サーバの機能としてリバースプロキシサーバ３０への接続を起動時に行う必要があるため、このときにリバースプロキシサーバ３０側で管理サーバの送信元ＩＰアドレスを手がかりに管理サーバとしての接続の許可・不許可を決めるようにすれば、内部ネットワークセグメント１つにつき１台管理サーバとして機能させることができる。
【００５１】
図８は、上記のようにして内部ネットワークセグメント５０に複数の管理サーバが設定されないように制御するためのシーケンス図である。ここでは、管理サーバが未だ設定されていないときに、ホストＰＣ５２とホストＰＣ５３がほぼ同時に起動された場合を例に説明する。
【００５２】
先ず、ホストＰＣ５２が起動してブロードキャストパケットを送信したあと直ぐにホストＰＣ５３が起動してブロードキャストパケットを送信したとすると、ホストＰＣ５２に対して応答がないまま一定期間を経過したあと、ホストＰＣ５２は、リバースプロキシサーバ３０に対して接続を試み、接続が許可されて管理サーバとして動作を開始する。一方、ホストＰＣ５３に対しても応答がないまま一定期間を経過するため、ホストＰＣ５３は、リバースプロキシサーバ３０に対して接続を試みるが、既に管理サーバとして接続許可されたホストＰＣ５２があるため接続が不許可とされ、ブロードキャストパケットを再度送信することとなる。再度送信したブロードキャストパケットに対してはホストＰＣ５２から応答があるため、管理サーバとしてのホストＰＣ５２との接続を行い、データ送信を行うこととなる。
【００５３】
上記のように、ホストＰＣが、起動時に問い合わせ用のブロードキャストパケットを送信し、ブロードキャストパケットを送信したあと一定期間が経過するまでに管理サーバとして機能している他のホストＰＣからの応答がなかった場合、リバースプロキシサーバ３０に対して管理サーバとしての接続依頼を行う構成としたので、内部ネットワークセグメント５０ごとに必要な管理サーバを事前に決定することなくホストＰＣのどれか一台に管理サーバ機能を割り当てることができ、常時管理サーバが立ち上がっているかどうかを確認する必要をなくすことができる。
【００５４】
なお、上述した実施の形態においては特に言及していないが、ネットワーク接続管理システムを構成する各部は、各部に搭載されている処理プログラム（ネットワーク接続管理プログラム）に従って、上述した各種の処理を実行する。
【図面の簡単な説明】
【００５５】
【図１】本発明の一実施形態に係るネットワーク接続管理システムの構成の例を示すブロック図である。
【図２】リバースプロキシサーバ、管理サーバ、およびホストＰＣの内部機能を説明するためのブロック図である。
【図３】ホストＰＣデータＤＢに格納されているホストＰＣデータの例を示す説明図である。
【図４】接続管理処理の例を示すフローチャートである。
【図５】ホストＰＣ上で稼動する既存のサーバプログラムへの接続方法の例を示すブロック図である。
【図６】管理サーバ決定処理の例を示すフローチャートである。

【図７】探索用パケット応答処理の例を示すフローチャートである。
【図８】内部ネットワークセグメントに管理サーバを１つだけ設定するためのシーケンス図である。
【符号の説明】
【００５６】
１０…クライアント端末，２０…ファイアウォール，３０…リバースプロキシサーバ，４０…ＮＡＴルータ，５０…内部ネットワークセグメント，５１…管理サーバ，５２～５４…ホストＰＣ，６０…外部通信ネットワーク

【図１】



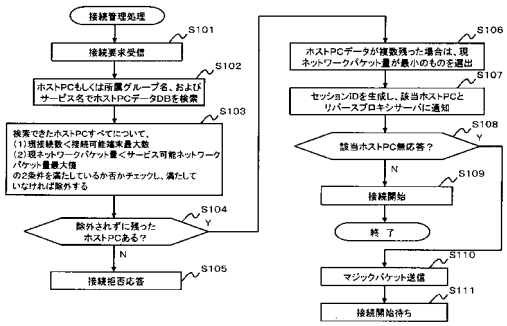
【図２】



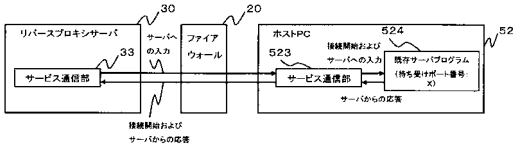
【図３】

ホストPC名
MACアドレス
IPアドレス
所属グループ名
提供可能サービス名
接続最大数orサービスID発行可能最大数
現在接続中のクライアント端末数
サービス可能ネットワークパケット量最大値
現ネットワークパケット量

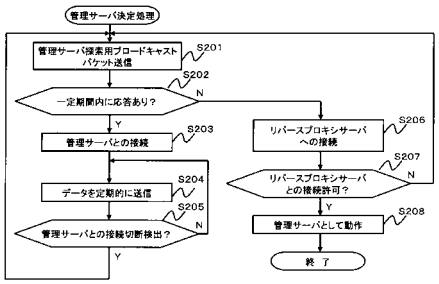
【図４】



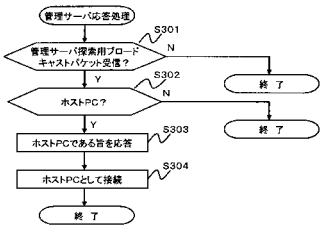
【図５】



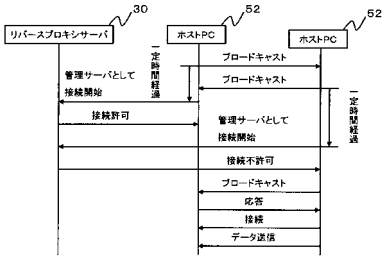
【図６】


管理サーバ決定処理
管理サーバ探索用ブロードキャストパケット送信
S201
S202
一定期間内に応答あり？
N
Y
S203
管理サーバとの接続
S204
データを定期的に送信
S205
管理サーバとの接続切断検出？
N
Y
S206
リバースプロキシサーバへの接続
S207
リバースプロキシサーバとの接続許可？
N
Y
S208
管理サーバとして動作
終了

【図７】


管理サーバ応答処理
S301
管理サーバ探索用ブロードキャストパケット受信？
N
Y
終了
S302
ホストPC？
N
Y
終了
S303
ホストPCである旨を応答
S304
ホストPCとして接続
終了

【図８】


30
52
52
リバースプロキシサーバ
ホストPC
ホストPC
一定時間経過
ブロードキャスト
ブロードキャスト
管理サーバとして接続開始
一定時間経過
接続許可
管理サーバとして接続開始
接続不許可
ブロードキャスト
応答
接続
データ送信

フロントページの続き

(56)参考文献　米国特許出願公開第２００４／００４９７０２（ＵＳ，Ａ１）
米国特許出願公開第２００６／００３１４４２（ＵＳ，Ａ１）
特開２００５－１００３４４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００