

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5054821号
(P5054821)

(45) 発行日 平成24年10月24日(2012.10.24)

(24) 登録日 平成24年8月3日(2012.8.3)

(51) Int.Cl.		F I	
HO 4 L 12/56	(2006.01)	HO 4 L 12/56	B
GO 6 F 15/00	(2006.01)	GO 6 F 15/00	4 2 O A
HO 4 L 12/66	(2006.01)	HO 4 L 12/66	A

請求項の数 39 (全 20 頁)

(21) 出願番号	特願2010-527990 (P2010-527990)	(73) 特許権者	500551079
(86) (22) 出願日	平成20年10月1日(2008.10.1)		ソニー コンピュータ エンタテインメン ト アメリカ リミテッド ライアビリテ イ カンパニー
(65) 公表番号	特表2010-541476 (P2010-541476A)		アメリカ合衆国、カリフォルニア州 94 4 0 4 - 2 1 7 5、フォスター・シティー 、セカンド・フロアー、イースト・ヒルス デイル・ブルバード 9 1 9
(43) 公表日	平成22年12月24日(2010.12.24)	(74) 代理人	100105924
(86) 国際出願番号	PCT/US2008/011415		弁理士 森下 賢樹
(87) 国際公開番号	W02009/045475		
(87) 国際公開日	平成21年4月9日(2009.4.9)		
審査請求日	平成22年8月24日(2010.8.24)		
(31) 優先権主張番号	60/997, 918		
(32) 優先日	平成19年10月5日(2007.10.5)		
(33) 優先権主張国	米国 (US)		
(31) 優先権主張番号	12/049, 954		
(32) 優先日	平成20年3月17日(2008.3.17)		
(33) 優先権主張国	米国 (US)		

最終頁に続く

(54) 【発明の名称】 NATタイプに基づくシームレスなホスト移行

(57) 【特許請求の範囲】

【請求項1】

ホストと複数のクライアントの間の接続を確立するステップであって、前記ホストと前記複数のクライアントの各々との間で交換されるデータが受領時に確認されるステップと、

前記ホストと前記複数のクライアント間の接続が確立したときに前記ホストと前記複数のクライアントとの間で共有されたNAT(Network Address Translation)プロファイル情報に少なくとも基づいて、前記複数のクライアントのうち第1クライアントのバックアップ実行可能性を判定するステップと、

前記第1クライアントに対してホスト情報を送信するステップであって、前記第1クライアントは少なくとも前記ホスト情報に基づき前記複数のクライアントのうち他のすべてのクライアントへの接続を確立し、前記ホストと前記複数のクライアントのうちの第2クライアントとの間で通信が中断された場合、前記第1クライアントが前記第2クライアントからデータを受け取るステップと、

を含むネットワークデータ分配を維持する方法。

【請求項2】

前記ホストと前記複数のクライアント間の前記NATプロファイル情報を共有するのに先立って、STUNサーバを通じてNATプロファイル情報を収集するステップをさらに含むことを特徴とする請求項1に記載の方法。

【請求項3】

クライアント - サーバ構成を利用して前記ホストと前記複数のクライアント間で前記 NAT プロファイル情報が共有されることを特徴とする請求項 1 に記載の方法。

【請求項 4】

ピアツーピア構成を利用して前記ホストと前記複数のクライアント間で前記 NAT プロファイル情報が共有されることを特徴とする請求項 1 に記載の方法。

【請求項 5】

前記 NAT プロファイル情報を用いて前記複数のクライアントから前記クライアントそれぞれに優先度を割り当てるステップをさらに含み、

NAT プロファイル情報に少なくとも基づいて前記複数のクライアントのうち第 1 クライアントのバックアップ実行可能性を判定するステップは、前記優先度の使用を含むことを特徴とする請求項 1 に記載の方法。

10

【請求項 6】

前記第 1 クライアントの優先度が、前記複数のクライアントのうちの他のクライアントに割り当てられた優先度と等しい優先度のとき、優先度の衝突を解決するステップをさらに含むことを特徴とする請求項 5 に記載の方法。

【請求項 7】

前記優先度の衝突を解決するステップは、前記第 1 クライアントのより高次の序数に対して前記複数のクライアントのうちの前記他のクライアントに割り当てられた序数を参照するステップをさらに含み、

前記序数はあらかじめ前記複数のクライアントそれぞれに割り当てられていることを特徴とする請求項 6 に記載の方法。

20

【請求項 8】

前記複数のクライアントの前記 NAT プロファイル情報は NAT タイプを含み、

前記 NAT プロファイル情報に少なくとも基づいて前記複数のクライアントのうち第 1 クライアントのバックアップ実行可能性を判定するステップは、前記 NAT タイプの使用を含むことを特徴とする請求項 1 に記載の方法。

【請求項 9】

前記複数のクライアントそれぞれの前記 NAT プロファイル情報は、NAT が UPnP (Universal Plug and Play) をサーボとするか否かに関する情報を含み、

前記 NAT プロファイル情報に少なくとも基づいて前記複数のクライアントのうち第 1 クライアントのバックアップ実行可能性を判定するステップは、NAT が UPnP をサーボとするか否かに関する情報の使用を含むことを特徴とする請求項 1 に記載の方法。

30

【請求項 10】

前記複数のクライアントそれぞれの前記 NAT プロファイル情報は、NAT のポート予測可能性に関する情報を含み、

前記 NAT プロファイル情報に少なくとも基づいて前記複数のクライアントのうち第 1 クライアントのバックアップ実行可能性を判定するステップは、前記ポート予測可能性の情報の使用を含むことを特徴とする請求項 1 に記載の方法。

【請求項 11】

前記複数のクライアントそれぞれの前記 NAT プロファイル情報は、NAT のポート保存に関する情報を含み、

前記 NAT プロファイル情報に少なくとも基づいて前記複数のクライアントのうち第 1 クライアントのバックアップ実行可能性を判定するステップは、前記ポート保存の情報の使用を含むことを特徴とする請求項 1 に記載の方法。

40

【請求項 12】

前記通信の中断は、前記第 2 クライアントが前記ホストにデータを送信した後のある時間内に前記ホストから前記第 2 クライアントに対して確認がないことにより認識されることを特徴とする請求項 1 に記載の方法。

【請求項 13】

前記ホストと前記複数のクライアントの各々との間の接続を判定するために前記複数の

50

クライアントにポーリングすることをさらに含む請求項 1 に記載の方法。

【請求項 1 4】

前記中断された通信が、前記ポーリングの結果によって示されることを特徴とする請求項 1 3 に記載の方法。

【請求項 1 5】

前記ホストから前記複数のクライアントの各々に対し、前記中断された通信に関する表示が送信されることをさらに含む請求項 1 に記載の方法。

【請求項 1 6】

前記中断された通信に基づき、前記ホストと前記第 2 クライアントとの間の通信を終了することをさらに含む請求項 1 に記載の方法。

10

【請求項 1 7】

前記第 1 クライアントのバックアップ実行可能性の判定が、該第 1 クライアントの帯域を判定することを含む請求項 1 に記載の方法。

【請求項 1 8】

前記第 1 クライアントのバックアップ実行可能性の判定が、前記第 1 クライアントが前記複数のクライアントのうちの他のクライアントの各々へと接続可能であるかを判定することをさらに含む請求項 1 に記載の方法。

【請求項 1 9】

前記第 1 クライアントへのホスト情報の送信が、該ホスト情報を提供するアプリケーションを送信することを含む請求項 1 に記載の方法。

20

【請求項 2 0】

前記ホストと前記複数のクライアント間の接続が確立したときに前記ホストと前記複数のクライアントとの間で共有された NAT プロファイル情報に少なくとも基づいて、前記複数のクライアントのうちの第 3 クライアントのバックアップ実行可能性を判定し、

少なくともホスト情報と NAT プロファイル情報とに基づき、前記第 3 クライアントが前記複数のクライアントのうちの他のすべてのクライアントへと接続し、かつ、前記第 1 クライアントと前記第 2 クライアントとの間の通信が中断された場合に該第 3 クライアントが前記第 2 クライアントからデータを受信できるように、前記第 3 クライアントに対してホスト情報を送信することをさらに含む請求項 1 に記載の方法。

【請求項 2 1】

30

前記ホストとの接続が確立される順序に少なくとも基づき、前記第 3 クライアントヘデータを送信する前に前記第 1 クライアントにデータを送信するように前記第 2 クライアントがさらに構成されていることを特徴とする請求項 2 0 に記載の方法。

【請求項 2 2】

前記第 1 クライアントの帯域と前記第 3 クライアントの帯域とに少なくとも基づき、前記第 3 クライアントにデータを送信する前に前記第 1 クライアントにデータを送信するように前記第 2 クライアントがさらに構成されていることを特徴とする請求項 2 0 に記載の方法。

【請求項 2 3】

複数のクライアントに接続されるよう構成され、該複数のクライアントの各々からデータを受け取りデータの受信を確認するホストと、

40

ホスト情報を受け取るように構成され、前記ホストと前記複数のクライアント間の接続が確立したときに前記ホストと前記複数のクライアントとの間で共有された NAT プロファイル情報に少なくとも基づいて、前記複数のクライアントのうちの他のすべてのクライアントと接続する第 1 クライアントと、

前記ホストとの間の通信が中断した場合に、前記第 1 クライアントに対してデータを送信するように構成された第 2 クライアントとを備え、

前記ホストは、第 1 クライアントのバックアップ実行可能性を交渉することを特徴とするネットワークデータ分配を維持するシステム。

【請求項 2 4】

50

前記通信の中断が、前記第2クライアントが前記ホストにデータを送信した後ある時間内に前記ホストからの確認がないことによって示されることを特徴とする請求項23に記載のシステム。

【請求項25】

前記第2クライアントは、前記ホストに対しデータを再送信するようにさらに構成されていることを特徴とする請求項23に記載のシステム。

【請求項26】

前記第2クライアントは、前記ホストと第2クライアントの間の通信の中断に関する情報を、前記複数のクライアントの各々に通知するようにさらに構成されていることを特徴とする請求項23に記載のシステム。

10

【請求項27】

前記第2クライアントは、前記ホストと第2クライアントの間の接続を停止するようにさらに構成されていることを特徴とする請求項23に記載のシステム。

【請求項28】

前記ホストは、接続に関する情報を前記複数のクライアントにポーリングするようにさらに構成されていることを特徴とする請求項23に記載のシステム。

【請求項29】

前記ホストは、該ホストと前記第2クライアントの間の通信の中断に関する情報を、前記複数のクライアントの各々に通知する通知するようにさらに構成されていることを特徴とする請求項23に記載のシステム。

20

【請求項30】

前記ホストは、該ホストと前記第2クライアントの間の接続を停止するようにさらに構成されていることを特徴とする請求項29に記載のシステム。

【請求項31】

前記ホストは、前記第1クライアントの帯域に基づいて前記第1クライアントのバックアップ実行可能性の交渉をするようにさらに構成されていることを特徴とする請求項23に記載のシステム。

【請求項32】

前記ホストは、前記複数のクライアントのうちの他のクライアントの各々に対して前記第1クライアントが接続可能であるか否かに基づきバックアップ実行可能性をさらに交渉することを特徴とする請求項23に記載のシステム。

30

【請求項33】

前記ホストは、前記第1クライアントに対してホスト情報を送信するようにさらに構成されていることを特徴とする請求項23に記載のシステム。

【請求項34】

前記ホストは、前記複数のクライアントのうちの他のクライアントの各々に関する情報を提供するように構成されたアプリケーションを送信することで、前記ホスト情報を送信することを特徴とする請求項33に記載のシステム。

【請求項35】

前記複数のクライアントのうちの第3クライアントがホスト情報を受け取るように構成されており、これにより前記第3クライアントが、前記ホストと前記複数のクライアント間の接続が確立したときに前記ホストと前記複数のクライアントとの間で共有されたNATプロファイル情報に少なくとも基づいて、複数のクライアントのうちの他のすべてのクライアントと接続することを特徴とする請求項23に記載のシステム。

40

【請求項36】

前記第2クライアントは、前記第1クライアントと前記第2クライアントとの間の通信が中断している場合、前記第3クライアントにデータを送信するようにさらに構成されていることを特徴とする請求項35に記載のシステム。

【請求項37】

クライアントから受け取ったデータを確認する応答を送信するように構成された確認モ

50

ジュールと、

共有されたNAT(Network Address Translation)プロファイル情報に少なくとも基づいて、第1クライアントのバックアップ実行可能性を交渉するように構成された交渉モジュールと、

少なくともNATプロファイル情報に基づき複数のクライアントのうちの他のクライアントすべてに前記第1クライアントが接続して第2クライアントからデータを受け取るように、前記第1クライアントに対してホスト情報を提供するアプリケーションを送信するように構成されたバックアップアプリケーションモジュールと、

を備えることを特徴とする、ネットワーク内でデータ分配を維持するためのコンピューティングデバイス。

10

【請求項38】

プロセッサにより実行可能でありグループメッセージング方法を実行するプログラムが具現化されたコンピュータ可読の記録媒体であって、

前記プログラムは、

ホストと複数のクライアントの各々との間で交換されたデータが受領時に確認されるように、複数のクライアントにホストを接続し、

前記ホストと前記複数のクライアント間の接続が確立したときに前記ホストと前記複数のクライアントとの間で共有されたNAT(Network Address Translation)プロファイル情報に少なくとも基づいて、前記複数のクライアントとのうちの第1クライアントのバックアップ実行可能性を判定し、

20

少なくともホスト情報に基づき前記複数のクライアントのうちの他のクライアントすべてに前記第1クライアントが接続して、複数のクライアントのうちの第2クライアントから第1クライアントがデータを受け取るように、前記第1クライアントに対してホスト情報を送信することを含む記録媒体。

【請求項39】

前記プログラムは、前記ホストと前記第2クライアントの間の接続を停止するための実行可能な命令をさらに含むことを特徴とする請求項38に記載の記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

30

本発明は、一般にネットワークに関する。より具体的には、本発明はネットワークにおけるデータ分配およびNAT(Network Address Translation)の使用に関する。

【背景技術】

【0002】

ネットワークは、通信システムによって互いに接続されたコンピューティングデバイスのグループを含むことができる。ネットワーク内のコンピュータは、ネットワーク内の他のコンピュータと通信し、データを交換し、リソースを分け合うことができる。ネットワークの例には、パーソナルエリアネットワーク(PAN)、ローカルエリアネットワーク(LAN)、ワイドエリアネットワーク(WAN)が含まれる。

【0003】

40

様々なネットワーク構成が当分野で知られている。図1Aに示す従来のクライアント-サーバネットワークは、クライアント120A-Dに接続されたホスト110を含む。ホスト110は、ネットワークセッション130を確立し、多数のクライアントによるネットワークセッション130への参加およびその方法を制御し、クライアント120A-Dがネットワークセッション130に参加した後はクライアントによる相互対話の方法を制御する。ホスト110は一般に広い帯域と高い処理能力を持つので、ホスト110は、ネットワークセッション130内のすべてのクライアント120A-Dとのデータの管理および分配を行うことが可能である。このような構成では、特定のクライアント(例えばクライアント120D)からのデータは、ホスト110を通して他のクライアント(例えばクライアント120A-C)に分配される。例えば、クライアント120Dはホスト11

50

0 にデータを送信する。他のクライアント、例えばクライアント 1 2 0 A がデータを要求すると、ホスト 1 1 0 はそのデータをクライアント 1 2 0 A に送信する。

【 0 0 0 4 】

ホストに接続しているおかげで、クライアントは自身が必要とするデータのみを（ホストを介して）要求することができ、そのため、クライアントは不必要なデータを管理する必要がない。このような構成は、ネットワークセッション内で交換されるすべてのデータを効率的に管理する能力を持たないクライアントの間で共通であってもよい。これらのクライアントは、データを管理し分配するホストを必要とする。

【 0 0 0 5 】

ネットワークセッション内のデータの管理および分配をホストに管理させることの欠点は、ホストとセッションクライアントのいずれか一つとの間の通信に影響を与える接続問題が生じたとき、データが失われる恐れがあることである。この場合、特定クライアントからのデータをホストに送信することができない。そのデータはまた、ネットワーク内の他のクライアントにとっても利用不可能になる。例えば、クライアント 1 2 0 D が突然ホスト 1 1 0 から切断されたとする。クライアント 1 2 0 D がホスト 1 1 0 に送っていたはずの情報はホスト 1 1 0 に到達せず、結果として、その情報はネットワークの残り（すなわち、クライアント 1 2 0 A - C）には送信することができない。失われた情報により、ネットワークセッション 1 3 0 に混乱を引き起こすことがあり、他のクライアントの動作に影響を与える恐れがある。このことは、インタラクティブなネットワークゲームの場合には特に当てはまる。

【 0 0 0 6 】

P 2 P（peer-to-peer）通信でクライアント間の通信の確立を試みるとき、N A T（Network Address Translation）に関してさらなる問題が起こりうる。P 2 P 通信は一般にネットワークに接続されているクライアント装置間のダイレクトな通信のことをいう。限定されるわけではないが、V o I P（Voice over Internet Protocol）、ビットトレント（BitTorrent）送信、ビデオ送信、ファイル共有、データ共有、および個々のクライアントの帯域制限を超えないクライアント間でのダイレクトな伝送における他の種類のものが P 2 P の適用例として含まれる。

【 0 0 0 7 】

N A T プロトコルを用いることにより、複数のノードや計算機が単一のインターネットまたはローカルな I P（Internet Protocol）アドレスを共有しうる。一例としては、ローカルエリアネットワークは、公開されたグローバルアドレスを外部ネットワークトラフィックに使用しうるし、ひとつの（あるいは一組の）プライベートな I P アドレスを内部のネットワークトラフィックに使用しうる。ネットワーク内のほとんどのクライアントは中央サーバに接続されている。その中央サーバは N A T ファイアウォール（以後単に「N A T」という。）の内部に置かれている。一般的に、以下の 4 つの種類の N A T が知られている。すなわち、フルコーン（full cone）、制限コーン（restricted cone）、ポート制限（port restricted）、およびシンメトリック（symmetric）の 4 つである。

【 0 0 0 8 】

フルコーン N A T は同一の内部 I P アドレスおよびポートからの要求を全て取得し、それらを同一の外部 I P アドレスおよびポートにマップする。外部にある任意のホストは、マップされた外部 I P アドレスにパケットを送信することで、内部のホストにパケットを送信することができる。制限コーンの場合も、同一の内部 I P アドレスおよびポートからの全ての要求は同一の外部 I P アドレスおよびポートにマップされる。しかし、フルコーン N A T とは異なり、（I P アドレス X をもつ）外部のホストが内部ホストにパケットを送ることができるのは、内部ホストがその I P アドレス X にパケットを以前送信したことがある場合に限られる。

【 0 0 0 9 】

ポート制限 N A T は制限コーン N A T と似ているが、制限はポート番号も含む。具体的に、外部のクライアントが、ソース I P アドレス X およびソースポート P をもつパケット

10

20

30

40

50

を内部ホストに送ることができるのは、内部ホストが以前そのIPアドレスXおよびポートPからパケットを送ったことがある場合に限られる。最後の例であるシンメトリックNATは、同一の内部IPアドレスおよびポートから特定のデスティネーションIPアドレスおよびポートへの全ての要求は、同一の外部IPアドレスおよびポートにマップされる。もし、同じホストが同じソースアドレスおよびポートをもつが宛先が異なるパケットを送信する場合、異なるマッピングが用いられる。さらに、パケットを受信する外部ホストだけがUDP (User Data Protocol) パケットを内部ホストに送り返すことができる。

【発明の概要】

【発明が解決しようとする課題】

【0010】

したがって、ネットワークセッションの接続に関連する問題を解決し、セッション内で中断されないデータ交換を維持する、改善されたネットワークデータ分配システムおよび方法が当分野で必要とされている。このような文脈のもと、最適なP2Pネットワークを生成するために、P2Pネットワークにおけるホストは有益なNATプロファイルを持つことが望まれている。したがって、中央サーバに接続されているいくつかのクライアントの間で有益なNATプロファイルを持つホストを判定することが当分野でさらに必要とされている。

【課題を解決するための手段】

【0011】

本発明のシステムおよび方法は、ネットワークセッションがデータを失うことなくホストとクライアントの間での通信の中断を乗り越えることを可能にする、ネットワークデータ分配の維持を提供する。ホスト機能は、シームレスにかつデータを大きく損なうことなくクライアントに移行する。本発明の実施形態は、ネットワークセッションのためにバックアップホストとして機能する一つまたは複数のクライアントを備える。他のクライアントがホストに対しデータを送信すると、そのデータの一つまたは複数のバックアップホストにも送信する。例えば、ホストにデータを送信したクライアントが所定の期間内にデータの確認を受領しないことがある。そのクライアントは、ホストに対してデータを再送信するとともに、データをバックアップホストにも送信する。バックアップホストの判定は、ホストと複数のクライアントとの間で接続が確立されたときにそのホストとクライアントとの間で共有された(NAT)プロファイル情報に基づいてもよい。

【0012】

本発明の様々な実施形態は、ネットワークデータ分配方法を含む。この方法は、ホストをクライアントに接続し、クライアントがバックアップホストとして機能できるか否かを判定し、機能できる場合、そのクライアントに対してバックアップホストとして機能できるようにする特定の情報を送信することを含む。この判定はNATプロファイル情報を用いて行ってもよい。バックアップホストとして機能することには、他のクライアントがホストとの通信ができないときに、その他のクライアントからの情報を受け取ることが含まれる。本発明の一部の実施形態では、方法はさらに、ホストとクライアントの間の通信が中断したことを表し、ホストとその特定クライアントの間の接続を停止することを含む。

【0013】

本発明の様々な実施形態は、ネットワークデータ分配システムを含む。このシステムは、ホストと、バックアップホストとして機能可能である第1クライアントと、ホストおよび第2クライアントの間の通信が中断した時に第1クライアントに対してデータを送信可能な第2クライアントとを含む。本発明の一部の実施形態では、第2クライアントもまたバックアップホストとして機能することができる。本発明の一部の実施形態は、それぞれがバックアップホストとして機能するように構成された複数のクライアントを含むことができる。NATプロファイル情報がバックアップホストとして機能可能であるか否かの判定に用いられてもよい。

【0014】

ネットワーク分配システムで使用されるホストシステムも、本発明の実施形態で提供さ

10

20

30

40

50

れる。このホストシステムは、受信時にクライアント通信を確認する確認モジュールと、特定のクライアントがバックアップホストとして機能できるか否かを交渉する交渉モジュールと、ホスト情報を提供するアプリケーションをクライアントに配信するバックアップアプリケーションモジュールとを含む。本発明の一部の実施形態は、さらにホスト情報データベースとタイマとを含む。NATプロファイル情報が収集され、解析され、バックアップホストとして機能可能であるか否かの判定に利用されてもよい。

【0015】

本発明の一部の実施形態は、ネットワークデータ分配用のコンピュータ記録媒体および命令を含む。この命令は、ホストをクライアントに接続すること、NATプロファイル情報の使用を通じてバックアップホストとして機能可能であるクライアントと交渉すること、およびクライアントにホスト情報を送信してクライアントがバックアップホストとして機能開始できるようにすることを含む。

10

【図面の簡単な説明】

【0016】

【図1A】当技術分野で既知であるクライアント-サーバネットワーク構成を示す図である。

【図1B】一つのバックアップホストを有するネットワークデータ分配用の例示的なシステムを示す。

【図1C】いくつかのバックアップホストを有するネットワークデータ分配用の例示的なシステムを示す。

20

【図1D】NATを利用するネットワークデータ分配用の例示的なシステムを示す。

【図2】ネットワークデータ分配システムにおいてシームレスなホスト移行を提供するコンピューティングデバイスの例示的な構成を示す図である。

【図3A】ネットワークデータ分配用の、ネットワークアドレス変換器を含むシステムの例示的な実装を示す図である。

【図3B】ネットワークデータ分配用の、例ネットワークアドレス変換器を含むシステムの別の実装例を示す図である。

【図4】NATプロファイル情報の使用を含むネットワークデータ分配の例示的な方法を示す図である。

【発明を実施するための形態】

30

【0017】

本発明はネットワークデータ配布システムおよび方法を含む。本発明の実施形態により、ホスト移行をシームレスに発生させることが可能になる。ホストとクライアントとの間で通信が中断した場合に、データを大きく損なうことなくネットワークセッションを継続することができる。ネットワークセッションのホストは、複数のクライアントに接続されていてもよい。これらクライアントの一つ（または複数）が、バックアップホストとして機能できるようにしてもよい。バックアップ実行可能性はクライアントと交渉され、ホスト情報はクライアントに送信される。このクライアントは続いてバックアップホストとして機能することができる。バックアップホストは、続いてネットワークセッション内の他のクライアントに接続し、他のクライアントからデータを受け取ってもよい。その後、ホストと特定クライアントとの間の通信が中断した場合、その特定クライアントは、自身のデータをバックアップホストに送信することができ、これによってデータを失うことなくネットワークセッションを継続することができる。

40

【0018】

全体を通して特定される構成要素は例示であり、様々な代替物、等価物または派生物を含む。ハードウェア、ソフトウェア、およびコンピュータで実行可能な命令の様々な組み合わせを利用することができる。プログラムモジュールおよびエンジンは、プロセッサによって実行されるときに特定タスクの実行をするルーチン、プログラム、オブジェクト、コンポーネントおよびデータ構造を含んでもよい。このプロセッサは、汎用のものでもまたはアプリケーション専用のものでよい。コンピュータ可読媒体に格納された、コンピ

50

ユータで実行可能な命令および関連するデータ構造とは、本明細書で開示された方法のステップを実行するか、および/または本明細書で開示された特定のシステム構成を実装するためのプログラミング手段の例を表している。

【0019】

図1Aに示され、また上で詳細に説明したクライアント-サーバネットワーク構成においては、各クライアントは、ネットワークセッション内のすべてのデータを処理する必要はない。代わりに、各クライアントは、そのクライアントがネットワークセッションに参加するために必要なデータのみを受け取り、それを処理する。一部のクライアントは、データのすべてを効率的に管理することができないが、これは、例えば帯域の不足か処理能力の不足によるものである。しかしながら、クライアントの中には、ネットワークセッション内のすべてのデータを管理する能力を有しているものもある。これらの特定のクライアントは、ネットワークセッションから得られるデータの一部またはすべてを格納するバックアップホストとして機能することができる。

10

【0020】

図1Aのシステム構成と比較して、図1Bは、一つのバックアップホストであるクライアント160Aを備えた、ネットワークデータ分配用の例示的なシステムを示している。バックアップホストは、ネットワークセッションのホストの機能の一部またはすべてを実行することが可能である任意のクライアントであってもよい。ネットワークセッション150のホスト140が実行不可能であるかまたは実行しないとき、ホスティング責任の一部またはすべてがバックアップホストに移行することができる。バックアップホストとしての資格を得るためには、バックアップの実行可能性を明示する候補ホスト(クライアント)が必要となる。バックアップ実行可能性を明示することには、例えば、帯域、処理能力、メモリ、ハードウェアまたはソフトウェア構成、あるいはサービス品質に関する一つ以上の要件を満足することを含む。クライアントのバックアップ実行可能性は、ホストとの交渉を通じて判定されてもよい。

20

【0021】

バックアップ実行可能性に関連しそれを確認する交渉が完了した後、ネットワークセッション150を通じてホスト140とクライアント160Aとの間でホスト情報が送信される。ホスト情報は、ネットワーク名、ネットワーク内でのクライアントのインターネットプロトコル(IP)アドレス、ファイアウォール情報、およびクライアント160Aがあるホスト責任を引き継ぐ必要がある場合の特定の責任に関する情報を含むことができる。ホスト情報を使用して、クライアント160Aは、ホスト140と他のクライアント160B-Dとの間の一つ以上の接続が中断した場合に、バックアップホストとして機能することが可能になる。例えば、クライアント160Bがホスト140から切断されるとすると、図3Aおよび図3Bに示されているように、クライアント160Bはクライアント160Aにデータを転送してもよい。ホスト140からクライアント160Aにホスト責任を移行することによって、クライアント160Bからの情報がネットワークセッション150で完全に失われることはない。

30

【0022】

一部の実施形態では、二つ以上のクライアントがバックアップホストとして機能可能であってもよい。図1Cは、いくつかのバックアップホストであるクライアント190A-Dを有するネットワークデータ配布用の例示的なシステムを示す。図1Cのネットワークセッション180内の各クライアントは、元のホスト170が利用できなくなった場合に、特定のバックアップホスト責任に関与することができる。例えば、クライアント190Aが得点の記録に責任を持つ一方で、クライアント190Bはゲーム環境内の状況変化に責任を持つことができる。クライアント190Cは参加基準(例えば、誰がゲームに参加できるか)について責任を持ち、クライアント190Dはチャット機能の責任を持つことができる。代わりに、クライアント190Aが上述のタスクのすべてについて責任を持ち、他のクライアント190B-Dは、クライアント190Aがその後機能しなくなった場合にそれらのタスクを引き継いでよい。

40

50

【 0 0 2 3 】

図 1 D は、N A T を利用するネットワークデータ分配用の例示的なシステムを示す。ネットワーク上のクライアント 1 9 5 A、クライアント 1 9 5 B、クライアント 1 9 7、およびクライアント 1 9 5 D は始め、外部ネットワーク 1 9 9 内のサーバ 1 9 1 に接続されている。サーバ 1 9 1 は、外部ネットワーク 1 9 9 に接続されているクライアント 1 9 5 A、クライアント 1 9 5 B、クライアント 1 9 7、およびクライアント 1 9 5 D 間で行われているゲームを監視する。

【 0 0 2 4 】

クライアント 1 9 5 A、クライアント 1 9 5 B、クライアント 1 9 7、およびクライアント 1 9 5 D はそれぞれ、対応するネットワークアドレス変換器 (N A T) 1 9 2 A、1 9 2 B、1 9 2 C、および 1 9 2 D の後ろに置かれている。各 N A T は、L A N (Local Area Network) の使用を可能とするインターネットの標準にしたがって、内部トラフィック用にあるプライベート I P アドレスのセットと外部トラフィック用に別のグローバル I P アドレスのセットとを用いるように構成されている。ほとんどの N A T は、動的な I P アドレス変換を実行し、そのため内部ネットワークが通信を初期化する前には外部ネットワークが内部ネットワークに到達する方法はない。しかし、クライアント 1 9 5 A、クライアント 1 9 5 B、クライアント 1 9 7、およびクライアント 1 9 5 D はサーバ・クライアントの関係を構築するため、クライアント 1 9 5 A、クライアント 1 9 5 B、クライアント 1 9 7、およびクライアント 1 9 5 D とサーバ 1 9 1 との間の通信は、N A T 1 9 2 A、1 9 2 B、1 9 2 C、および 1 9 2 D によって制限されない。

【 0 0 2 5 】

クライアント同士がダイレクトに通信することができる P 2 P ネットワークを確立する際、あるクライアントはホスト 1 9 7 として確立する。これにより他のピア 1 9 5 (P 2 P ネットワークと接続しているクライアントであってホストでないクライアント) は互いにダイレクトに接続する。ピア 1 9 5 は、完全結合グリッド (Fully Connected Grid ; F C G) として知られる形態で接続される。ホスト 1 9 7 は、各クライアントの N A T プロファイルに基づいて判定される。N A T 1 9 2 A、1 9 2 B、1 9 2 C、および 1 9 2 D は、上述の 4 つの異なる N A T タイプ (フルコーン、制限コーン N A T、ポート制限コーン、およびシンメトリック) のうちのひとつであってもよい。

【 0 0 2 6 】

一般に、フルコーン、制限コーン、およびポート制限コーンの通過は、シンメトリック N A T を通過する場合よりも複雑である。クライアントがシンメトリック N A T の後ろに置かれる場合の N A T 通過の実装は、米国特許出願番号第 1 1 / 2 4 3 , 8 5 3 号に記載されている。この開示は既に参照により援用されている。具体的には、ある N A T の後ろに置かれたクライアントが、その N A T 上で予測されたトランスポートアドレスのリストの構築を含むポート予測を実行する。その後、クライアントは第 1 のノードから第 2 のクライアントに対し、予測されたトランスポートアドレスのリストを含む招待メッセージを送信する。次いで、シンメトリック N A T の後ろに置かれたクライアントは、予測されたトランスポートアドレスを用いて第 2 のノードとの接続性のチェックを実行する。接続性のチェックは、S T U N (Simple Traversal of UDP through NAT) リクエストを予測されたトランスポートアドレスそれぞれに並列に送信することによって実行される。シンメトリック N A T の後ろに置かれたクライアントがそのリクエストを受信すると、そのクライアントは第 2 のクライアントに S T U N 応答を送信する。第 2 のクライアントが S T U N 応答を受信した場合、そのアドレスに情報を送信することを開始できる。

【 0 0 2 7 】

上述の 4 つ以外の N A T タイプを設けてもよい。ある場合には、標準的な技術を用いて N A T を通過することができる。他の場合には、N A T の振る舞いが予測できない状態が不安定な状態のため、そのような N A T の後ろに置かれたクライアントとの通信は信頼性に欠く。ホスト 1 9 7 は、他のピア 1 9 5 A、1 0 5 B、および 1 9 5 D との間で情報の通信をすることが任務であるから、通信能力の妨げにならないタイプの N A T の背後にあ

10

20

30

40

50

ることが重要である。ピア195A、195B、195D、およびホスト197が完全結合グリッド内に置かれているような例において、あるNATの後ろに置かれたホストがそのNATの通信能力の影響を受けないことが特に望まれる。

【0028】

最も好ましいNATプロファイルを持ったホスト197を選択することで、より信頼できるP2P通信が得られる。ひとたびホスト197が確立されると、ピア195群は最初にホスト197に情報を送信し、次いでホスト197がその情報を受信者であるピア195に中継することによって、ピア195群は相互に通信することができる。ダイレクトな通信パスを確立するためにホスト197を使った後は、クライアントは直接情報を送信する。

10

【0029】

本発明のある実施の形態では、クライアント195A、195B、および197は、外部ネットワーク199と関連づけられているSTUNサーバ193を通してNATプロファイル情報を取得する。STUNサーバ193は、NATの後ろに置かれているIPが使用可能なクライアントが、そのNATの存在およびNATタイプを探知することを許可するための軽量プロトコルを利用する。STUNサーバ193は、ほとんどの種類のNATと共に動作し、NATの特定の挙動にも依存しない。ある観点から見れば、STUNサーバ193は、クライアント195Aに立てかけられたミラーのように作用し、クライアント195Aは、自身のローカルな送信アドレスがどのようにパブリックな送信アドレスにマップされるかを見ることができる。NAT192Aの後ろに置かれたクライアント195Aは、STUNサーバ193との通信を通して、NAT192Aのタイプを判定することができる。

20

【0030】

クライアント195A、195B、197、および195Dはそれぞれ、STUNサーバ193を使ってNATプロファイル情報を取得し、取得した情報を中央サーバ191に中継する。これにより中央サーバ191が、どのクライアントが最もホスト197に適しているかを定めることができる。同様に、いずれかのクライアント195A、195B、197、195Dは、STUNサーバ193を使ってNATプロファイル情報を取得し、P2Pネットワークを通して通信を試みる他の全てのクライアントにその情報を中継してもよい。これにより、クライアント195A、195B、197、および195Dが、ホスト197を最もよく判定することができる。

30

【0031】

サーバ191に接続されている各クライアントは、P2Pネットワーク内で使用するための自身のNATプロファイル情報を収集する。このプロファイル情報には、クライアントの前方にあるNATタイプに関する情報、そのNATがUPnP(Universal Plug and Play)をサポートするか否かに関する情報、そのNATがポート保存を提示するか否かに関する情報、およびそのNATがポートの予測可能性をサポートしているか否かに関する情報が含まれる。

【0032】

本願において「ポート保存」とは、ひとたびある内部IPアドレスが特定の外部ポートにマップされると、一貫してその特定のポートにマップされることを意味する。同様に、「ポートの予測可能性」とは、たとえ常に同じポートにマップされるものではないとしても、ある内部IPアドレスがマップされる外部ポートを予測することができることを意味する。例えば、外部のポート番号は、内部IPアドレスのそれぞれのマッピングが試みられると一貫して増加されてもよい。

40

【0033】

各クライアント用のNATプロファイル情報は、P2P通信のためのホストを最もうまく選択するために、サーバに接続されている全てのクライアントに関する優先度のリストを生成するために使われる。潜在的なホスト間の優先順位が同順位である場合は、どの潜在的なホストを現実のホストとして選択するかを決定するために序数を設定しておいても

50

よい。ある実施の形態では、そのような序数はサーバによって割り当てられてもよい。たとえば、クライアントがサーバに接続された順にする。あるいは、分散調停アルゴリズムを用いて、2以上の等しく適切な潜在的なホストの中から一つのホストを選択してもよい。最初のホストがP2Pネットワークを離れることを決定するか、P2Pネットワークから何らかの理由で接続が切られることがあった場合、この情報はP2Pネットワーク用の次のホストを選択するために用いられる

【0034】

ひとたびNATプロファイル情報が所定のクライアントによって収集されると、そのクライアント用のNATプロファイルはサーバに接続している他のクライアントに共有される。P2Pの分散を通して、あるいはクライアントからサーバを通して、残りのクライアントへの分散が生ずる。サーバは専用のネットワーク接続を通してプロファイル情報を分散する。ひとたび全てのNATプロファイルがクライアントによって提出されると、どの特定のクライアントがホストやピアとなるべきか、あるいはそれらが全体としてネットワークの交流のための条件を満たしていないかどうかの判定がなされる。上述の各クライアントが取得したプロファイル情報に基づいて、この判定はなされる。

10

【0035】

例えば、複数の要因に基づいて優先度が割り振られることにより、最も好適なプロファイルを持っているクライアントに基づいて、有効なクライアントの中からひとつのホストが選択できる。残りのクライアントはそれらのプロファイル情報に基づいて、ピアに割り当てられるか、あるいはピアまたはホストとして認識されずに終わる。例えば、通過可能でないNATの後に置かれたクライアントは、ピアまたはホストとしてネットワークに接続するために必要な条件を満たさない。

20

【0036】

典型的な優先順位付けスキームは、5つの分離された区分に分けることができる。アクティブ、起こりうる、不明、進行中、非アクティブの5つである。「アクティブ」タグはそのクライアントがホストとして非常によい候補であることを示す。「起こりうる」タグはそのクライアントがホストとしてよい候補であるが、アクティブタグの付いたクライアントの方が優先することを示す。「不明」タグは、その特定のクライアントがホストとしてよい候補であるか否かをネットワークが判定できないことを示す。「進行中」タグは、そのクライアントがホストとしてよい候補であるか否かをネットワークが判定中であることを示す。最後に、「非アクティブ」タグは、クライアントがホストとしての任務を担うことができないことを示す。

30

【0037】

優先度タグは、以下の4つの典型的な基準に基づく。すなわち、NATタイプ、UPnP (Universal Plug and Play) 機能、ポート保存、およびポート予測の4つである。他のいくつかの要因も優先度の判定に用いてもよい。これらの要因はクライアントのサービス品質のプロファイルに該当し、ピングタイム、バンド幅の振る舞い、地理、レイテンシ、およびIPプロバイダを含むがこれらに限定されない。

【0038】

図2は、ネットワークデータ配布システムにおいてシームレスなホスト移行を提供するコンピューティングデバイスの構成の一例200を示す。ホスト200は、ネットワーク内で中央通信ハブとして機能することができ、例えばサーバなどのコンピューティングデバイスである。通常はクライアント動作のために用意されるコンピューティングデバイスは、ホスト200の構成の一部またはすべてを有していてもよいが、これは、ある時点においてはクライアントがバックアップホストとなることがあるという事実のためである。ホスト200は、ネットワークインタフェース210、確認モジュール220、交渉モジュール230、ホスト情報データベース240、バックアップアプリケーションモジュール250、ポーリングモジュール260、タイマ270およびNATモジュール280を含むことができる。

40

【0039】

50

本発明で参照される場合、モジュール（またはアプリケーション）とは、様々なシステムレベルの機能を実行するルーチンの集合のことをいう。モジュールは、必要に応じて、ハードウェア（例えば情報処理装置など）およびデバイスドライバによって動的にロードおよびアンロード（例えば実行）される。本明細書で述べるモジュラーソフトウェアコンポーネントは、より大きなソフトウェアプラットフォームの一部として組み込まれてもよいし、あるいはアプリケーション専用コンポーネントの一部として統合されてもよい。

【0040】

ネットワークインタフェース210は、ネットワーク内でホストと他のコンピューティングデバイス間の通信が可能になるように構成された様々なハードウェアおよび/またはソフトウェアコンポーネントのうち任意のものであってよい。ネットワークインタフェース210は、有線、無線、および/またはインターネットベースの通信ネットワークを介して通信を行うコンポーネントを含んでもよい。

10

【0041】

確認モジュール220は、クライアントによって送信された情報がホスト200によって受信されたことを確認できるようにする。ネットワークインタフェース210を通じてホスト200がクライアントから情報を受け取ると、確認モジュール220は、情報を送信したクライアントに対して受信確認（ACK）を送信することができる。例えば、クライアントがホスト200に対してゲーム状態データの変更に関連する情報を送信する場合、確認モジュール220は送信クライアントに対して、その情報が受信されたことを表すACK返答を送信することができる。確認モジュール220により送信されたACK返答は、受信した情報の内容およびその情報の量に関する表示、および/または情報が破損していたり不完全であったりした場合にはその旨の表示をさらに含むことができる。

20

【0042】

送信クライアントによる特定のデータ送信に対してACKを受領していないということは、データ送信がホスト200によって受け取られていないことを表す。ホスト200がデータ送信（またはその一部）を受け取っていないということは、ホスト200とデータ送信をしたクライアントとの間の接続に問題があるか、またはホスト200自体に問題があることを示している。特定の数のデータ送信がホスト200からのACK返答の受信をしていない場合、送信クライアントは移行動作を実行してもよく、これによって、ホスト機能の一部またはすべてがバックアップホストに移行される。

30

【0043】

交渉モジュール230は、様々なパラメータに基づきクライアントのバックアップ実行可能性を交渉する。例えば、実行可能なバックアップホスト/クライアント候補は、ある量の利用可能な帯域を有している必要があるかもしれない。クライアントの帯域は、ネットワークセッションにおけるデータのすべてをクライアントが管理できるよう十分なものである必要がある。バックアップ実行可能性は、クライアントが関連する様々なサービス基準の品質に準拠している必要があるかもしれない。例えば、pingレート、パケットロス、利用可能なメモリ、プロセッサ速度等である。

【0044】

交渉モジュール230は、クライアント候補がネットワーク内の他の各クライアントと接続可能であるかについて判定してもよい。実行可能なバックアップホストは、ネットワーク内の他の各クライアントと接続可能であり、かつ情報を受け取ることができる必要がある。バックアップ実行可能性のパラメータは、ネットワークセッションのタイプによって判別されてもよい。例えば、特定のゲームネットワークセッションは、ゲーム環境内で多くの状態変化が生じるので、バックアップ実行可能とするために特定の量の帯域とプロセッサ速度とを必要とする場合がある。単純なファイル転送のような複雑さの少ないランザクションでは、より小さな帯域および/または処理能力を必要とする。

40

【0045】

交渉モジュール230は、複数のクライアントとともにバックアップ実行可能性について交渉するように構成されていてもよい。これによって、一連のバックアップホストを生

50

じさせる。代わりに、交渉モジュール 230 は、特定のタスクに対するバックアップ責任をクライアントのグループの間で割り当てるように構成されていてもよい。一連のバックアップホストを提供することによって、ネットワークまたはホスト/クライアント条件が保証するとき、ホスティングの義務を、ホストから第 1 のバックアップホストへ、第 2 のバックアップホストへ、といったようにシームレスに移行させることができる。バックアップホスト責任および/または特定の責任の順序は、クライアントがホストに接続されている順序に基づいて割り当てられてもよい。代わりに、帯域やサービス品質などの他の要因に基づいて、順序および/または責任が定められてもよい。

【0046】

ホスト情報データベース 240 は、ホスト、クライアント、またはネットワークセッションに関連する情報を格納することができる。ホスト情報データベース 240 に格納される情報により、コンピューティングデバイスは、ネットワークセッション内の他のクライアントへの接続などの特定のホスティング義務を果たすことが可能になる。このようなホスト情報は、ネットワーク名、ネットワーク内のクライアントのインターネットプロトコル (IP) アドレス、およびファイアウォール情報を含んでもよい。ネットワークからクライアントが切断されたりまたはネットワークに新たなクライアントが参加したりといったイベントが生じると、ホスト情報データベース 240 が更新されてもよい。例えば、新たなクライアントの IP アドレスは、ホスト情報データベース 240 に追加される必要がある。

【0047】

ホスト情報データベース 240 とともに動作して、バックアップアプリケーションモジュール 250 は、クライアントにダウンロードされ、インストールされ、実行されることができるアプリケーションを作成する。このアプリケーションは、基礎的な実行可能要件を満足することに加えて、クライアントがバックアップホストとして動作するために必要である特定の機能をクライアントに提供する。アプリケーションは、クライアントがネットワークセッション内の他のクライアントと接続しデータを交換できるようにクライアントを調整することができる。

【0048】

オプションであるポーリングモジュール 260 は、ネットワークセッション内のすべてのクライアントにポーリングをするように構成される。ポーリングモジュール 260 を使用して接続するクライアントをポーリングすることができる。接続のポーリングには、ネットワークセッション内の各クライアントに対して小さなデータパケットを送信すること、データパケットを受け取ったクライアントからの返信/確認を受け取ること、およびホスト 200 との通信に問題を抱えているクライアントを判定することを含むことができる。

【0049】

ポーリングモジュール 260 は、周期的な間隔で自動的にクライアントにポーリングすることができる。ポーリングモジュール 260 は、新たなクライアントがネットワークセッションに参加したりあるいは接続が中断した事象があったり (例えば、クライアントがホスト 200 により送信されたデータを確認していない) といったイベントが生じたときに、クライアントに対しポーリングをするように構成することもできる。ポーリングモジュール 260 のポーリング動作は、米国特許公開番号第 2003-0204566 号の「マルチユーザアプリケーションインタフェース」に記載されているような周期的な鼓動にも似ているかもしれない。この開示は既に参照により援用されている。

【0050】

ホスト 200 はタイマ 270 を含んでもよい。タイマ 270 は、イベント後に経過した時間を測定するように構成されている。ホスト 200 はタイマ 270 を使用して、ポーリングモジュール 260 により生成されるようなデータ送信と、そのデータ送信の確認との間の時間を判定することができる。この種の情報を使用して、特定クライアントへの接続を打ち切るか否かの判定をすることができる。タイマ 270 により測定するとき、ホスト

10

20

30

40

50

200がある期間の間、特定のクライアントからの確認を受け取っていないかまたはポーリングの応答を受け取っていない場合、ホスト200はそのクライアントとの接続を停止することができる。

【0051】

バックアップアプリケーションモジュール250により作成されたアプリケーションは、ポーリングモジュール260およびタイマ270の機能と似た特定の機能をさらに含んでもよい。ネットワークセッションから特定クライアントを外すか否かを判定しようとするホスト200とは異なり、この「鼓動」機能はバックアップホストとして指定されたクライアントによって使用され、ホスト200が特定のホスト義務を実行できなくなったり、またはホスト義務の実行に連続して失敗した時間を判定する。ホスト200が特定の義務を実行不可能であるかまたは実行に失敗したということは、確認モジュール220により生成されるACKすなわち鼓動を連続して受け取っていないことで表すことができる。

10

【0052】

ホスト200はNATモジュール280を含む。NATモジュール280の実行によりNATプロファイル情報の収集、共有、および受信が可能となる。同様に、NATモジュール280の実行により、NATプロファイル情報を用いてネットワーク内の最も実行可能なホストを判定することが可能となる。NATプロファイル情報はメモリ、専用のデータベース、またはホスト情報データベース240のような他のデータベースに格納される。

【0053】

ホスト200（および他の多くのクライアント）は、ネットワークアドレス変換器の後ろに存在し、そのネットワークアドレス変換器は、特定の計算機のために、内部のIPアドレスをパブリックなIPアドレスに変換する。パブリックなIPアドレスはネットワーク内の他の計算機から見られるアドレスである。ある実施の形態では、ホスト200や他の計算機はネットワークアドレス変換器を内包する。しかしながら、あるネットワークでは、NATが全く使用されない。NATプロファイル情報は、使用されている（もしあれば）NATタイプ、NATがUPnP（Universal Plug and Play）を行う能力、NATのポート保存を維持する能力、およびNATのポート予測についての情報を含む。

20

【0054】

場合によっては、ホスト200（またはネットワーク内の他の計算機）は、サービス情報の等価性のような付加的な情報に基づいて、補助的な調停フィルタを適用し、2以上の同程度に有望な候補デバイスの中からホストデバイスを選ぶ決定を調停することが望ましい。サービス品質情報は、クライアントのピングタイム、帯域幅の振る舞い、地理、レイテンシ、IPプロバイダなどの要因や上述の他の要因を含んでもよい。これらの追加的な情報はメモリや（専用または他の）データベースに格納される。

30

【0055】

図3Aは、ネットワークアドレス変換器（図示せず）を含むネットワークデータ分配用の例示的なシステム300の実装を示す。ホスト200は複数のクライアント310A-Dに接続されている。クライアント310Aは、ホスト200とのバックアップ実行可能性についての交渉を成功させており、接続320を通じてホスト情報を受け取っている。ホスト情報を使用して、クライアント310Aはネットワーク内の他のクライアント、すなわちクライアント310B-Dと接続する。接続330により、クライアント310B-Dはクライアント310Aと直接（すなわち、ホスト200を介することなく）通信する。クライアント310B-Dは、それぞれのクライアントからホスト200へのデータ送信が困難になった場合に、接続330を用いてクライアント310Aとデータを交換することができる。クライアント310B-Dは、ホスト200とのデータ送信における問題に関係なく、クライアント310Aに対して自動的にデータを送信することもできる。

40

【0056】

図3Bは、ネットワークアドレス変換器（図示せず）を含むネットワークデータ分配用の例示的なシステムの別の実装を示す。特に、図3Bは、ホスト200とクライアント3

50

10 Dとの間の通信が中断した場合の、ネットワークデータ分配用の例示的なシステムを表している。具体的には、ホスト200とクライアント310 Dの間のデータ送信340が失敗した様子が示されている。クライアント310 Dがホスト200に対するデータ送信340を実行しようと試みている一方で、障害のある接続のためにホスト200による送信の受け取りが妨げられている。

【0057】

クライアント310 Aはネットワークセッションのバックアップホストであるので、クライアント310 Dは、ホスト200に向けられたのと同じデータを、バックアップデータ送信350で直接(すなわち、ホスト200を介さずに)クライアント310 Aに送ることができる。続いて、クライアント310 Aは、データ送信360でホスト200に対してそのデータを送る。この特定の実施形態では、クライアント310 Dとホスト200とを分離する障害のある通信のために、クライアント310 Aは、クライアント310 Dとホスト200の間のプロキシ(代理)として機能する。続いて、ホスト200は、クライアント310 Aを介して受け取ったものではあるが、クライアント310 Dからのデータをクライアント310 Bと310 Cに分配する。代わりに、クライアント310 Dとホスト200の間の接続に対するホスト義務をホスト200が維持することができなかった場合に、クライアント310 Aがデータをクライアント310 Bまたは310 Cに送信してもよい。

10

【0058】

ホスト200とクライアント310 Dの間の通信が中断したので、クライアント310 Dはクライアント310 Aを介してセッションデータを取得する必要がある。クライアント310 Aは、いずれかのコンピューティングデバイスに代わってデータを要求することに加えて、ホスト200およびクライアント310 Dに対するデータ送受信の中間媒体として機能することができる。

20

【0059】

図4は、NATプロファイル情報の利用を含むネットワークデータ分配をする例示的な方法400を示すフローチャートである。図4で特定されるステップ(およびその順序)は例示であり、様々な代替物、等価物または派生物を含むことができ、またその実行の順序に限定されない。図4のプロセスのステップ(およびその様々な代替物)は、プロセッサにより実行可能である命令を含む機械可読媒体またはコンピュータ可読記録媒体(例えば、光ディスク、メモリカードまたはハードドライブ)を含む、ハードウェアまたはソフトウェアで実現可能である。

30

【0060】

ステップ410で、ホスト(例えばホスト200)がネットワークセッションを確立する。ホストは、ネットワークセッションを進行させる様々な態様の他に、ネットワークセッションに参加可能な対象についての特定のパラメータを設定してもよい。ホストは、特定のクライアントのみまたは招待されたクライアントのみが参加できるプライベートなネットワークセッションを確立することができる。代わりに、ホストは、公衆に開かれており任意のクライアントが参加可能であるネットワークセッションを確立することができる。

40

【0061】

ステップ420で、ホストに接続することによって複数のクライアントがネットワークセッションに参加する。ネットワークセッションに参加可能である対象に関する特定のパラメータをホストが設定していた場合、ホストへの接続またはネットワークセッションへの参加が許可される前に、クライアントはそれらのパラメータを満足している必要がある。

【0062】

ステップ430で、図2の交渉モジュール230を介してバックアップ実行可能性が交渉される。一つまたは複数のクライアントが、バックアップホストとして機能するための能力およびリソースを有する、実行可能なバックアップホストとなることができる。帯域

50

およびサービス品質を含むバックアップ実行可能性の様々な側面が評価され、特定のクライアントがバックアップホストとして機能可能であるか否かが判定される。NATプロファイル情報も同様に考慮される。交渉モジュール230の要件に応じて、ネットワークセッション内のクライアント中に一つまたは二つ以上の実行可能なバックアップホストが存在するか、またはバックアップホストが存在しないこともある。

【0063】

ステップ440で、バックアップ責任が割り当てられる。実行可能なバックアップホストであるクライアントが複数ある場合、順序および/または特定の責任に関して、それらのクライアントの間でバックアップ責任を割り当てる必要がある。ネットワークセッション内のクライアントは、第1の実行可能なバックアップホストに対して自身のデータを送信することができる。第1の実行可能なバックアップホストは、ホストによって特定されるか、またはブロードキャストあるいは他の通信によって最初にバックアップと見なされたものである。後者については、米国特許公開番号第2003-0217135号の「動的プレイヤー管理」に例証されており、この開示は既に参照により援用されている。第1の実行可能なバックアップホストがバックアップホストとして動作不可能であるか、または動作不可能になった場合、他のクライアントは、第2の実行可能なバックアップホストに対して自身のデータを送信して、ネットワークセッションに参加することができる。本明細書に開示の、および/または上述の「動的プレイヤー管理」の出願に開示されている手段を利用して、第2のバックアップホストと通信する必要性を示すことができる。

【0064】

ステップ450で、ネットワークセッション内の他の各クライアントに対して特定のクライアントが接続可能であるか否かが判定される。バックアップホストは、セッション内の各クライアントおよびあらゆる他のクライアントと接続可能である必要がある。第1のクライアントが第2のクライアントと接続できない場合、第1のクライアントとは、ネットワークセッションのバックアップホストとして機能することはできない。例えば、第1クライアントによるあるタイプの接続を妨げるファイアウォール問題を第1のクライアントが有しているかもしれない。潜在的なバックアップホストがいかなる理由によっても別のクライアントと接続できない場合、本方法はステップ440に戻りバックアップ責任を再割り当てする。

【0065】

あるクライアントが実行可能なバックアップホストであり、ネットワークセッション内の他のクライアントのすべてと接続可能であると判定されると、方法はステップ460に進む。ステップ460で、バックアップ情報が実行可能なバックアップホストにダウンロードされる。バックアップ情報をバックアップホストに提供することで、ホストはネットワークから抜け出すことができ、バックアップホストは、ネットワークセッション内の他のクライアントにより要求されるあらゆる情報を提供できるようになる。図2のバックアップアプリケーションモジュール250の文脈で述べたように、バックアップ情報は、シームレスなホスト移行を容易にするアプリケーションのダウンロードおよびインストールの一部として提供することができる。

【0066】

ステップ470で、ネットワークデータ分配が開始される。図3Aに示したように、ホストとクライアントの間でデータ送信が発生する。図3Bにさらに示したように、二つのクライアントの間、すなわちホスト接続問題を抱えるクライアントから、バックアップホストとして動作可能であるクライアントに対してデータ送信が行われる。さらに、バックアップホストは、ホストに向けてデータを送るか、または要求に応じて他のクライアントに対して直接データを送ることができる。データを中継しなければならないあらゆる接続を介して、そのデータを要求するコンピューティングデバイスに対してデータが提供される。

【0067】

例示的な実施形態を参照して本発明を説明してきたが、当業者ならば、本発明の真の精

10

20

30

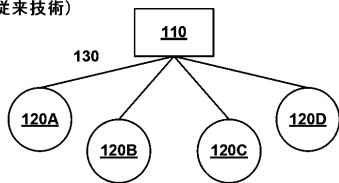
40

50

神および範囲を逸脱することなく、様々な変更が可能であり、また等価物による要素の置換が可能であることを理解するだろう。加えて、本発明の本質的な教示を逸脱することなく修正が可能である。本明細書で述べた様々な方法を実装するために様々な代替システムを利用することができ、また上述のシステムから生じる特定の結果を達成するために様々な方法を使用することができる。

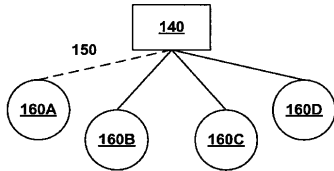
【図 1 A】

(従来技術)



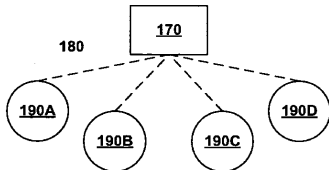
【図 1 B】

FIGURE 1B

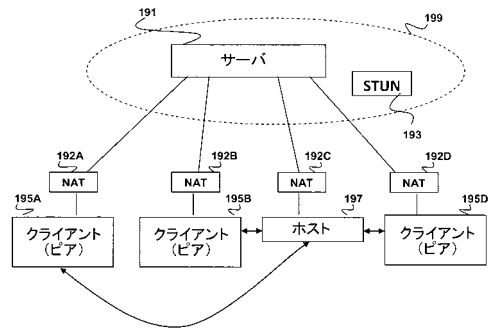


【図 1 C】

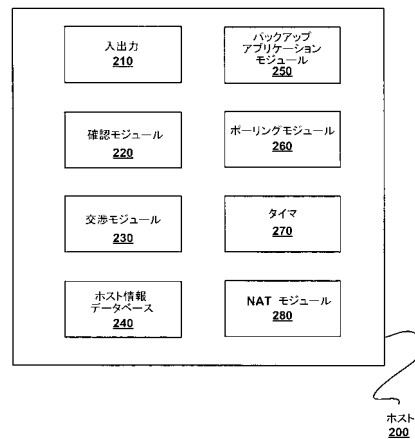
FIGURE 1C



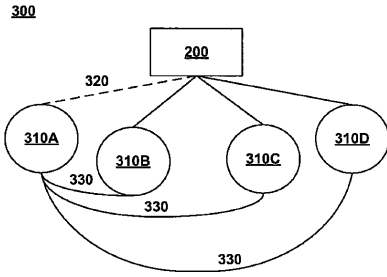
【図 1 D】



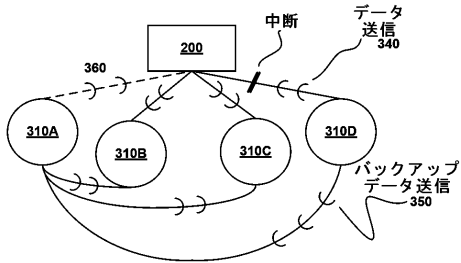
【図 2】



【 図 3 A 】
FIGURE 3A

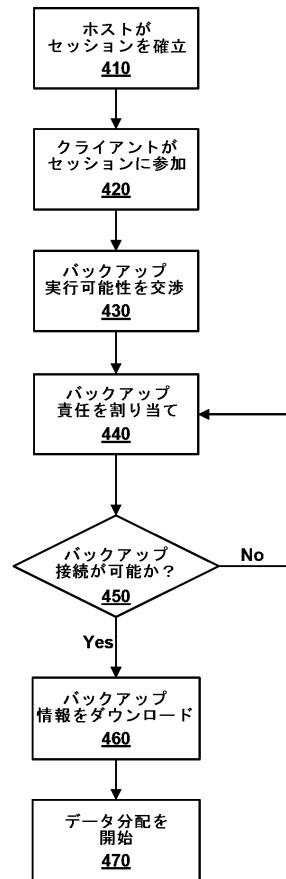


【 図 3 B 】



【 図 4 】

400



フロントページの続き

(31)優先権主張番号 12/235,438

(32)優先日 平成20年9月22日(2008.9.22)

(33)優先権主張国 米国(US)

(72)発明者 ロイ、ロナルド、ジェー、

アメリカ合衆国、カリフォルニア州 94404-2175、フォスター・シティー、セカンド・フロアー、イースト・ヒルズデイル・ブルバード 919、ソニー・コンピュータ・エンタテインメント・アメリカ・インク内

(72)発明者 ジェイコブ、マーク、エル、

アメリカ合衆国、カリフォルニア州 94404-2175、フォスター・シティー、セカンド・フロアー、イースト・ヒルズデイル・ブルバード 919、ソニー・コンピュータ・エンタテインメント・アメリカ・インク内

(72)発明者 ハリス、アダム、ピー、

アメリカ合衆国、カリフォルニア州 94404-2175、フォスター・シティー、セカンド・フロアー、イースト・ヒルズデイル・ブルバード 919、ソニー・コンピュータ・エンタテインメント・アメリカ・インク内

審査官 中木 努

(56)参考文献 特開2000-215177(JP,A)

特開2006-157941(JP,A)

特開2006-295909(JP,A)

特開2005-151142(JP,A)

特開2005-107819(JP,A)

特開2004-180003(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/56

H04L 12/66

H04L 12/46

G06F 15/00

G06F 13/00