

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第4909026号
(P4909026)

(45) 発行日 平成24年4月4日(2012.4.4)

(24) 登録日 平成24年1月20日(2012.1.20)

(51) Int.Cl.

F 1

H04L 12/66 (2006.01)
H04L 12/46 (2006.01)H04L 12/66
H04L 12/46A
A

請求項の数 9 (全 25 頁)

(21) 出願番号 特願2006-315714 (P2006-315714)
 (22) 出願日 平成18年11月22日 (2006.11.22)
 (65) 公開番号 特開2008-131464 (P2008-131464A)
 (43) 公開日 平成20年6月5日 (2008.6.5)
 審査請求日 平成21年11月6日 (2009.11.6)

前置審査

(73) 特許権者 000001007
 キヤノン株式会社
 東京都大田区下丸子3丁目30番2号
 (74) 代理人 100126240
 弁理士 阿部 琢磨
 (74) 代理人 100124442
 弁理士 黒岩 創吾
 (72) 発明者 安間 健介
 東京都大田区下丸子3丁目30番2号キヤ
 ノン株式会社内
 審査官 中木 努

最終頁に続く

(54) 【発明の名称】受信装置、方法、及び、プログラム

(57) 【特許請求の範囲】

【請求項 1】

L A N に接続される受信装置であって、
 前記 L A N と W A N に接続される中継装置の前記 W A N 側に存在する送信装置から送信された送信データを前記 L A N を介して受信する受信手段と、
 前記中継装置が前記受信手段への送信データを識別するための W A N 側のポート番号、及び、前記受信手段が前記送信装置から送信された送信データを識別するための前記 L A N 側のポート番号を前記中継装置に設定する設定手段と、
 前記 W A N とは異なる媒体を介して前記送信装置に入力される前記中継装置の W A N 側の I P アドレス及び前記 W A N 側のポート番号を出力する出力手段とを有し、

前記受信手段は、入力された前記 W A N 側の I P アドレス及び前記 W A N 側のポート番号を用いて前記受信装置にアクセスする前記送信装置から送信され、前記中継装置により前記受信手段の L A N 側の I P アドレス及び前記 L A N 側のポート番号を付与されて中継された送信データを、前記 L A N 側の I P アドレス及び前記 L A N 側のポート番号により識別して受信することを特徴とする受信装置。

【請求項 2】

請求項 1 の受信装置において、
 前記設定手段は、前記 L A N 側の I P アドレスを前記中継装置に設定することを特徴とする受信装置。

【請求項 3】

10

20

請求項 1 又は 2 の受信装置において、
前記設定手段は、前記WAN側のIPアドレスを前記中継装置に設定することを特徴とする受信装置。

【請求項 4】

LANに接続される受信装置における受信方法であって、
受信手段が、前記LANとWANに接続される中継装置の前記WAN側に存在する送信装置から送信された送信データを前記LANを介して受信する受信ステップと、

設定手段が、前記中継装置が前記受信手段への送信データを識別するためのWAN側のポート番号、及び、前記受信手段が前記送信装置から送信された送信データを識別するための前記LAN側のポート番号を前記中継装置に設定する設定ステップと、

出力手段が、前記WANとは異なる媒体を介して前記送信装置に入力される前記中継装置のWAN側のIPアドレス及び前記WAN側のポート番号を出力する出力ステップとを有し、

前記受信ステップでは、前記受信手段が、入力された前記WAN側のIPアドレス及び前記WAN側のポート番号を用いて前記受信装置にアクセスする前記送信装置から送信され、前記中継装置により前記受信手段のLAN側のIPアドレス及び前記LAN側のポート番号を付与されて中継された送信データを、前記LAN側のIPアドレス及び前記LAN側のポート番号により識別して受信することを特徴とする受信装置における受信方法。

【請求項 5】

請求項 4 の受信方法において、
前記設定ステップでは、前記設定手段が、前記LAN側のIPアドレスを前記中継装置に設定することを特徴とする受信方法。

【請求項 6】

請求項 4 又は 5 の受信方法において、
前記設定ステップでは、前記設定手段が、前記WAN側のIPアドレスを前記中継装置に設定することを特徴とする受信方法。

【請求項 7】

LANに接続され、前記LANとWANに接続される中継装置の前記WAN側に存在する送信装置から送信された送信データを前記LANを介して受信する受信手段を有するコンピュータに、

前記中継装置が前記受信手段への送信データを識別するためのWAN側のポート番号、及び、前記受信手段が前記送信装置から送信された送信データを識別するための前記LAN側のポート番号を前記中継装置に設定する設定手順と、

前記WANとは異なる媒体を介して前記送信装置に入力される前記中継装置のWAN側のIPアドレス及び前記WAN側のポート番号を出力する出力手順と、

入力された前記WAN側のIPアドレス及び前記WAN側のポート番号を用いて前記受信装置にアクセスする前記送信装置から送信され、前記中継装置により前記受信手段のLAN側のIPアドレス及び前記LAN側のポート番号を付与されて中継された送信データを、前記LAN側のIPアドレス及び前記LAN側のポート番号により識別して受信するよう前記受信手段を制御する受信制御手順とを実行させるためのプログラム。

【請求項 8】

請求項 7 のプログラムにおいて、
前記設定手順では、前記LAN側のIPアドレスを前記中継装置に設定することを特徴とするプログラム。

【請求項 9】

請求項 7 又は 8 のプログラムにおいて、
前記設定手順では、前記WAN側のIPアドレスを前記中継装置に設定することを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

10

20

30

40

50

【0001】

本発明は、受信装置方法、及び、プログラムに関する。

【背景技術】**【0002】**

送信装置から受信装置にインターネットを介してデータを送信する場合、そのデータは、受信装置をインターネットに接続するためのルーターにより中継される場合がある。

【0003】

また、受信装置は、セキュリティなどの点から、受信を制限（場合によっては、禁止）することが望ましい場合がある。

【0004】

さらに、特許文献1には、シードサーバントのサーバントIDおよび自サーバントのサーバントIDを利用し、論理ネットワークへの参加要求および参加受付を行う方法が提示されている。この方法では、論理ネットワークへの参加要求の送信先であるシードサーバントのサーバントIDおよび自サーバントIDを予め設定する。

【特許文献1】特開2005-94264号公報

10

【発明の開示】**【発明が解決しようとする課題】****【0005】**

従来は、データが受信装置に受け取られるようにするための情報（例えば、受信装置のIPアドレス、ポート番号、識別子、認証情報など）を、送信装置に設定する必要があった。

20

【0006】

このような情報の設定は、煩雑かつ困難であるという問題があった。特に、ユーザーインターフェースの貧弱なカメラ等の小型携帯機器では、多くの入力を伴う前記設定を行うことは困難であり、非常に不便であるという問題があった。

同様に、受信の制限、禁止の設定も、煩雑かつ困難であるという問題があった。

【0007】

本発明は、簡単に、データ送信、あるいは、受信制限の設定を行うことのできる受信装置方法、及び、プログラムを提供することを目的とする。

【課題を解決するための手段】

30

【0008】

本発明の受信装置は、LANに接続される受信装置であって、前記LANとWANに接続される中継装置の前記WAN側に存在する送信装置から送信された送信データを前記LANを介して受信する受信手段と、前記中継装置が前記受信手段への送信データを識別するためのWAN側のポート番号、及び、前記受信手段が前記送信装置から送信された送信データを識別するための前記LAN側のポート番号を前記中継装置に設定する設定手段と、前記WANとは異なる媒体を介して前記送信装置に入力される前記中継装置のWAN側のIPアドレス及び前記WAN側のポート番号を出力する出力手段とを有し、前記受信手段は、入力された前記WAN側のIPアドレス及び前記WAN側のポート番号を用いて前記受信装置にアクセスする前記送信装置から送信され、前記中継装置により前記受信手段のLAN側のIPアドレス及び前記LAN側のポート番号を付与されて中継された送信データを、前記LAN側のIPアドレス及び前記LAN側のポート番号により識別して受信することを特徴とする。

40

【発明の効果】**【0016】**

本発明は、中継装置が受信手段への送信データを識別するためのWAN側のポート番号、及び、受信手段が前記送信装置から送信された送信データを識別するためのLAN側のポート番号を中継装置に設定する設定手段を有し、受信手段が、入力されたWAN側のIPアドレス及びWAN側のポート番号を用いて受信装置にアクセスする送信装置から送信され、中継装置により受信手段のLAN側のIPアドレス及びLAN側のポート番号を付

50

与されて中継された送信データを、 LAN 側の IP アドレス及び LAN 側のポート番号により識別して受信することにより、煩雑、困難な設定なく、 WAN から受信装置にアクセスする送信装置から送信された送信データを、中継装置を介して受信することができる。

【発明を実施するための最良の形態】

【0024】

<実施形態 1 >

以下、本実施形態について、図面を参照して詳細に説明する。

【0025】

本実施形態のネットワークシステムの構成について、図 1 を参照して説明する。

10

図 1 において、 100 は、インターネットである。インターネット 100 は、単一の Wide Area Network (WAN) 、 Local Area Network (LAN) 、アドホックネットワークなどのネットワークで実現してもよい。またインターネット 100 は、必要に応じた複数の WAN 、 LAN 、アドホックネットワークの複合で構成されてもよい。また、本実施形態におけるインターネットは一例であり、他の通信ネットワーク、乃至、通信ネットワークの複合でも良い。ある形態では、ネットワーク制御装置 101A とインターネット 100 の間 103 には、ホームルーターが存在する。

101A 、 B は、論理ネットワークの制御を行うネットワーク制御装置（送信装置、受信装置、通信装置）である。

【0026】

20

102 は、近距離無線通信による通信可能な記憶メディア（媒体）である。記憶メディアは、他の通信手段による通信（例えば、 Universal Serial Bus (USB) 、 Wireless Universal Serial Bus (WUSB) ）で構成されていてもよい。赤外線通信でもよい。また、記憶メディアは、記憶装置を保持する通信装置で構成されていてもよい。また、本実施形態における記憶メディアは一例であり、記憶装置の複合でもよい。

【0027】

図 1 には、ネットワーク制御装置 101A 、 B が 2 台接続されているが、 2 台に制限されず、 3 台以上接続されていてもよい。

【0028】

30

本実施形態のネットワーク制御装置 101A 、 B について、図 2 を参照して説明する。なお、ネットワーク制御装置 101A 、 B は、 PC (パーソナルコンピュータ) などのコンピュータシステムには、限られない。例えば、ネットワーク制御装置 101A 、 B は、コンピュータを内蔵したテレビ等の各種家電製品、通信機能を有するゲーム機、携帯電話、等を含む。すなわち、ネットワーク制御装置 101A 、 B は、他のネットワーク制御装置と通信するための通信機能を有する端末、または、これらの組合せによって実施可能である。

【0029】

201 は、コンピュータシステムの制御をつかさどる中央演算装置（以下 CPU と記す）である。

40

【0030】

202 は、ランダムアクセスメモリ（以下 RAM と記す）であり、 CPU 201 の主メモリとして、及び実行プログラムの領域や該プログラムの実行エリアならびにデータエリアとして機能する。

【0031】

203 は、 CPU 201 の動作処理手順を記録しているリードオンリーメモリー（以下 ROM と記す）である。 ROM 203 には、コンピュータシステムの機器制御を行うシステムプログラムである基本ソフト（ OS ）を記録したプログラム ROM と、システムを稼動するために必要な情報などが記録されたデータ ROM がある。 ROM 203 の代わりに後述の HDD 209 を用いる場合もある。

50

【0032】

204は、ネットワークインターフェース（以下NETIFと記す）であり、ネットワークを介してコンピュータシステム間のデータ転送を行うための制御や接続状況の診断を行う。NETIF204は、インターネット100を介した通信、及び、記憶メディア102との通信を行う。

【0033】

205は、ビデオRAM（以下VRAMと記す）であり、コンピュータシステムの稼動状態を示す後述するCRT206の画面に表示される画像を展開し、その表示の制御を行う。

【0034】

206は、表示装置であって、例えば、ディスプレイである。以下CRTと記す。

【0035】

207は、後述する外部入力装置208からの入力信号を制御するコントローラである。

【0036】

208は、コンピュータシステムの利用者がコンピュータシステムに対して行う操作を受け付けるための外部入力装置であり、例えば、キーボードなどである。

【0037】

209は、記憶装置を示し、例えば、ハードディスク（HDD）などである。アプリケーションプログラムや、画像情報などのデータ保存用に用いられる。本実施形態におけるアプリケーションプログラムとは、本実施形態を構成する各種セキュリティプロトコル制御手段を実行するソフトウェアプログラムなどである。

【0038】

210は、外部入出力装置であって、例えばCD-ROMドライブなどの記憶媒体を入出力するものであり、上述したアプリケーションプログラムの媒体からの読み出しなどに用いられる。以下、FDDと記す。なお、HDD209に格納するアプリケーションプログラムやデータをFDD210に格納して使用することも可能である。

【0039】

200は、上述した各ユニット間の接続するための入出力バス（アドレスバス、データバス、及び制御バス）である。

【0040】

図2のネットワーク制御装置101Aは、受信装置である。NETIF204は、送信装置であるネットワーク制御装置101Bから送信され、ホームルーターにより中継された送信データを、伝送媒体であるインターネット100を介して受信する。さらに、NETIF204は、伝送媒体であるインターネット100とは異なる媒体である記憶メディア102に情報を出力する。また、CPU201は、後述するように、ネットワーク制御装置101Aをインターネット100に接続するための中継装置であるホームルーターの設定を行う。

【0041】

また、NETIF204は、後述するように、インターネット100上の通信装置であるSTUN（Simple Traversal of UDP through NAT）サーバー（不図示）から情報を受信する。

【0042】

NETIF204は、記憶メディア102から情報を入力する。一方、CPU201は、NETIF204によるデータ受信の制限を行う。

【0043】

また、図2のネットワーク制御装置101Bは、送信装置である。CPU201は、送信データを、NETIF204からネットワーク制御装置101Aに送信する。

【0044】

本実施形態のネットワーク制御装置（受信装置、送信装置、通信装置）101A、Bに

10

20

30

40

50

おけるモジュールの構成について、図3を参照して説明する。

【0045】

301は、ネットワーク制御部305に対する論理ネットワークの制御の指示、論理ネットワークの接続受付処理を行う制御部である。また、制御部301は、TCP/IP通信処理部302に対する論理ネットワークの接続設定情報の送信処理、TCP/IP通信処理部302に対する論理ネットワークの接続設定情報の受信処理を行う。さらには、制御部301は、NFC通信処理部303に対する論理ネットワークの接続設定情報の送信処理、NFC通信処理部303に対する論理ネットワークの接続設定情報の受信処理を行う。接続設定情報の詳細は、後述する。

【0046】

302は、TCP/IPの通信処理を行うTCP/IP通信処理部である。本実施形態では、TCP/IPの通信処理を例としているが、これに限らず、他の有線、無線の通信手段の処理で構成されていてもよい。

【0047】

303は、NFCの通信処理を行うNFC通信処理部である。本実施形態では、NFCの通信処理を例としているが、これに限らず、他の無線、有線の通信処理で構成されていてもよい。TCP/IP通信処理部302とNFC通信処理部303は、異なる媒体を介して、情報を送信、受信する。

【0048】

304は、論理ネットワークの接続受付情報および論理ネットワークの接続設定情報を保持する情報保持部である。論理ネットワークの接続受付情報および論理ネットワークの接続設定情報の詳細は、後述する。

305は、論理ネットワークの制御、管理を行うネットワーク制御部である。

【0049】

本実施形態は、論理ネットワークの形式に依存する部分が小さい。本実施形態では、論理ネットワークを、レイヤ3のVirtual Private Network (VPN)、レイヤ2のVPN、分散ハッシュテーブルによるネットワークで構成することができる。また、論理ネットワークは、Peer-to-Peer接続のネットワーク、アプリケーションレイヤのネットワーク等で構成することもできる。

【0050】

図3において、情報保持部304は、図1のRAM202に対応し、TCP/IP通信処理部302、NFC通信処理部303は、図1のNETIF204に対応する。図1において、TCP/IP通信処理部302に対応してNETIF204Aを設け、NFC通信処理部303に対応してNETIF204Bを設けても良い。また、図3において、制御部301及びネットワーク制御部305は、図2のCPU201に対応する。制御部301、ネットワーク制御部305は、それぞれ、CPU201の機能の一部に対応する。図3において、制御部301が、ネットワーク制御部305の機能を併せ持つようにしても良い。

【0051】

図3のネットワーク制御装置101Aは、受信装置である。この受信装置であるネットワーク制御装置101Aにおいて、TCP/IP通信処理部302は、送信装置であるネットワーク制御装置101Bから送信され、ホームルーターにより中継された送信データを、伝送媒体であるインターネット100を介して受信する。また、制御部301は、ネットワーク制御装置101Aをインターネット100に接続するための中継装置であるホームルーターの設定を行う。また、NFC通信処理部303は、インターネット100とは異なる媒体である記憶メディア102に情報を出力する。

【0052】

また、TCP/IP通信処理部302は、インターネット100上の通信装置であるSTUN (Simple Traversal of UDP through NAT) サーバー(不図示)から情報を受信する。

10

20

30

40

50

【0053】

NFC通信処理部303は、記憶メディア102から情報を入力する。そして、CPU201は、TCP/IP通信処理部302による送信データの受信を制限する。

【0054】

また、図2のネットワーク制御装置101Bは、送信装置である。CPU201は、TCP/IP通信処理部302から送信データをネットワーク制御装置101Aに送信する。

【0055】

図1において、ネットワーク制御装置(受信装置)101Aとネットワーク制御装置(送信装置)101Bが論理ネットワークを構成する例を説明する。図7において、ネットワーク制御装置101A、ネットワーク制御装置101B、記憶メディア102の情報要素の例について説明する。図7のネットワーク制御装置101A、ネットワーク制御装置101B、記憶メディア102は、図1のそれぞれに相当する。

10

【0056】

ネットワーク制御装置101Aは、記憶メディア102の接続を検出すると、記憶メディア102から接続設定情報を取得する。

【0057】

一方、記憶メディア102に、接続設定情報がない場合、ネットワーク制御装置101Aは、接続受付情報と接続設定情報を生成する。ネットワーク制御装置101Aは、生成した接続設定情報にて適合したネットワーク設定を行えるかの確認を行う。この確認の詳細は、後述する。その後、ネットワーク制御装置101Aは、生成した接続設定情報を、記憶メディア102に書き込む。次に、ネットワーク制御装置101Aは、論理ネットワークへの接続受付開始処理を行った後、論理ネットワークに接続されているネットワーク制御装置(不図示)に論理ネットワークへの接続受付開始を通知する。接続受付開始処理の詳細は、後述する。

20

【0058】

以上の一連の動作が終了した状態を、図7における状態(1)とする。図7における状態(1)では、ネットワーク制御装置101Aに接続受付情報が、記憶メディア102に接続設定情報が記録されており、ネットワーク制御装置101Bには情報(接続設定情報)がない。接続受付情報および接続設定情報の詳細は、後述する。

30

【0059】

ネットワーク制御装置101Aは、記憶メディア102の切断を検出すると、論理ネットワークの接続設定情報があるかの判定を行い、処理を終了する。この場合、接続設定情報はないので、処理を終了する。

【0060】

ネットワーク制御装置101Bは、記憶メディア102の接続を検出すると、記憶メディア103から接続設定情報を取得する。記憶メディア102に接続設定情報がある場合、ネットワーク制御装置101Bは、記憶メディア102から接続設定情報を読み出し、接続設定情報を記憶する。次に、ネットワーク制御装置101Bは、接続設定情報がネットワーク制御装置101B自身で生成されたものか判定する。

40

【0061】

接続設定情報がネットワーク制御装置101B自身で生成されたものでない場合、論理ネットワークへの接続を開始するか判定する。この接続設定情報に対応する論理ネットワークに接続していない場合、この論理ネットワークへの接続を開始する。論理ネットワークへの接続を開始する場合、論理ネットワークへの接続開始処理を行い、この論理ネットワークに接続されているネットワーク制御装置に論理ネットワークへ接続開始を通知する。この論理ネットワークに接続されているネットワーク制御装置は、ネットワーク制御装置101A及び不図示のネットワーク制御装置である。このように、ネットワーク制御装置101Bは、送信装置である。ネットワーク制御装置101Bは、記憶メディア102から接続設定情報を入力する。そして、ネットワーク制御装置101Bは、入力した接続

50

設定情報がネットワーク制御装置 101B 自身で生成されたものではない場合に、接続開始を通知する送信データに、宛先情報を付与して、送信する。この宛先情報は、記憶メディア 102 から入力した接続設定情報に含まれる。

【0062】

以上の一連の動作が終了した状態を、図 7 における状態 (2) とする。図 7 における状態 (2) では、ネットワーク制御装置 101A に接続受付情報が、ネットワーク制御装置 101B、および、記憶メディア 102 に接続設定情報が記憶されている。

【0063】

ネットワーク制御装置 101B は、記憶メディア 102 の切断を検出すると、論理ネットワークへ接続しているか判定する。論理ネットワークに接続中である場合、ネットワーク制御装置 101B は、論理ネットワークの接続を終了するか判定する。ユーザーインターフェースや他のプログラム等により、論理ネットワーク接続の継続が設定されなければ、接続を終了する。論理ネットワークの接続を終了する場合、ネットワーク制御装置 101B は、論理ネットワークの接続を終了し、この論理ネットワークに接続されているネットワーク制御装置に論理ネットワークからの切断を通知する。この論理ネットワークに接続されているネットワーク制御装置は、ネットワーク制御装置 101A 及び不図示のネットワーク制御装置である。その後、ネットワーク制御装置 2 は、記憶している接続設定情報を削除し、処理を終了する。

10

【0064】

以上の一連の動作が終了した状態を、図 7 における状態 (3) とする。図 7 における状態 (3) では、ネットワーク制御装置 101A に接続受付情報が、記憶メディア 102 に接続設定情報が記憶されており、ネットワーク制御装置 101B には情報 (接続設定情報) がない。

20

【0065】

ネットワーク制御装置 101A は、記憶メディア 102 の接続を検出すると、記憶メディア 102 から接続設定情報を取得する。記憶メディア 102 に、接続設定情報があり、記憶されている接続設定情報がネットワーク制御装置 101A で生成した接続設定情報である場合、接続設定情報を削除するか判定する。ボタン、プログラム等により、接続設定情報の削除が指示された場合、接続設定情報を削除する。接続設定情報を削除する場合、ネットワーク制御装置 101A は、対応するネットワーク設定をネットワーク制御装置 101A 内から削除し、記憶メディア 102 から対応する接続設定情報を削除する。ネットワーク制御装置 101A は、論理ネットワークの接続受付を終了し、ネットワーク制御装置 101A 内の接続受付情報を削除した (無効にした) 後、この論理ネットワークに接続されているネットワーク制御装置に論理ネットワークの接続受付終了を通知する。この論理ネットワークに接続されているネットワーク制御装置は、不図示のネットワーク制御装置である。以上の一連の動作が終了した状態を、図 7 における状態 (4) とする。図 7 における状態 (4) では、ネットワーク制御装置 101A に情報 (接続受付情報) なし、ネットワーク制御装置 101B に情報 (接続設定情報) なし、記憶メディア 102 に情報 (接続設定情報) なしとなる。

30

【0066】

このように、ネットワーク制御装置 101A は、送信装置であるネットワーク制御装置 101B に入力される接続設定情報を、記憶メディア 102 に出力し、ネットワーク制御装置 101B から送信された送信データを受信する。また、ネットワーク制御装置 101A は、記憶メディア 102 から接続設定情報を入力すると、接続受付を終了し、以降のインターネット 100 からのデータ受信を制限する。

40

【0067】

本実施形態のネットワーク制御装置 101A、B における記憶メディア接続検出時のシーケンスについて、図 4 のフローチャートを参照して説明する。図 4 は、HDD 209 又は FDD 210 に記憶されたコンピュータプログラムの一部を表わす。コンピュータである CPU 201 は、このプログラムを、HDD 209 又は FDD 210 から読み出して、

50

図4のフローチャートに対応する動作を行う。HDD209又はFDD210は、このプログラムを、CPU201が読み出すことができるよう記憶した記憶媒体である。

【0068】

ステップS401において、接続を検出した記憶メディア102に接続設定情報があるか判定する。ステップS401において、接続を検出した記憶メディア102に接続設定情報がない場合、ステップS402に進む。ステップS401において、接続を検出した記憶メディア102に接続設定情報がある場合、ステップS408に進む。

【0069】

ステップS402において、接続設定情報を生成するか判定する。論理ネットワークへの接続の受付を行うネットワーク制御装置（例えば、101A）では、制御部301が、接続生成情報を生成する機能を持ち、接続設定情報を生成する。一方、論理ネットワークへの接続の要求を行うが、論理ネットワークへの接続の受付を行わないネットワーク制御装置では、制御部301が、接続生成情報を生成する機能を持たないので、接続設定情報を生成しない。論理ネットワークへの接続の受付を行うネットワーク制御装置においては、制御部301に対する、ユーザーインターフェースや他のプログラムによって、接続設定情報の生成に関する指示を入力することにより、接続設定情報を生成するか否かの決定を行ってもよい。また、全てのネットワーク制御装置において、常に、接続情報を生成するようにしてもよい。この形態では、ステップS402の判定は、不要である。ステップS402において、接続設定情報を生成する場合、ステップS403に進む。ステップS402において、接続設定情報を生成しない場合、処理を終了する。

10

20

【0070】

ステップS403において、接続設定情報と、論理ネットワークへの接続を受付する接続受付情報を生成し、ステップS404に進む。本実施形態では、接続受付情報は、接続設定情報に対応した認証情報を持つ。論理ネットワークの接続設定情報には、論理ネットワークへの接続許可を行うノード（上述の例では、ネットワーク制御装置101A）のIPアドレス、ポート番号、プロトコル、認証方式、パスワードなどの情報が含まれる。接続許可を行うノードのIPアドレスは、マルチキャストアドレス、エニーキャストアドレスでもよい。また、ネットワーク制御装置が分散する場合、接続設定情報の生成を行うノードと異なるユニキャストアドレスでもよい。

30

【0071】

ステップS404において、論理ネットワークの接続設定情報に適合するネットワークの設定が可能かどうか判定する。ステップS404では、制御部301が、接続設定情報を受け付けるプログラムのポート番号が利用可能であるか否か、適合する認証方式を受け付けるか否かなどの判定を行う。また、ホームルーターのポート番号の設定を行えるか否かの判定を行う。ホームルーターは、図1の103に位置する。本形態では、ホームルーターはUPnPのInternet Gateway Deviceとして定義されているので、外部からのメッセージによりポート番号を変更できるか判定を行う事ができる。ステップS404において、論理ネットワークの接続設定情報に適合するネットワークの設定が可能である場合、ステップS405に進む。ステップS404において、論理ネットワークの接続設定情報に適合するネットワークの設定が不可能である場合、処理を終了する。

40

【0072】

ステップS405において、論理ネットワークの接続設定情報を記憶メディア102へ書き込み、ステップS406に進む。ステップS406において、論理ネットワークの接続受付の開始処理を行い、ステップS407に進む。この接続受付の開始処理では、制御部301は、論理ネットワークの接続受付を行うための待ち受けソケットを開く。

【0073】

また、ホームルーターのポート番号の設定を行う場合には、UPnPによるInternet Gateway DeviceにAdd Port Mappingを行い、UPnPによるInternet Gateway Deviceのポート番号の設定を行う。

50

このポート番号は、ステップ S 4 0 3 で生成した接続設定情報のポート番号である。Add Port Mapping の命令により、第 1 の IP アドレス、及び、ポート番号と、第 2 の IP アドレス、及び、ポート番号との変換の設定を行う。

【 0 0 7 4 】

ここで、変換が設定される第 1 の IP アドレス、及び、ポート番号は、ホームルーターの WAN (ネットワーク制御装置 101B) 側に公開するネットワーク制御装置 101A の IP アドレス、および、ポート番号である。ホームルーターは、Internet Gateway Device の機能を持つ。また、第 2 の IP アドレス、及び、ポート番号は、LAN (ネットワーク制御装置 101A) 側に公開するネットワーク制御装置 101A の IP アドレス、および、ポート番号である。したがって、ステップ S 4 0 3 で生成した接続設定情報のポート番号は、ホームルーターの WAN (ネットワーク制御装置 101B) 側のポート番号である。すなわち、接続設定情報に含まれるポート番号はホームルーターの WAN 側に公開するネットワーク制御装置の IP アドレス、および、ポート番号である。また、接続受付情報に含まれる IP アドレス、および、ポート番号は、ホームルーターの LAN (ネットワーク制御装置 101A) 側に公開するネットワーク制御装置の IP アドレス、および、ポート番号である。

【 0 0 7 5 】

すなわち、ネットワーク制御装置 101A は、受信装置であって、送信装置であるネットワーク制御装置 101B から送信された送信データを、伝送媒体であるインターネット 100 を介して受信する。そして、ネットワーク制御装置 101A は、以下の第 1 の識別情報、及び、第 2 の識別情報を、ネットワーク制御装置 101A をインターネット 100 に接続するホームルーター (中継装置) に設定する。

【 0 0 7 6 】

ここで、第 1 の識別情報は、ホームルーター (中継装置) が、ネットワーク制御装置 101A (の TCP / IP 通信処理部 302) への送信データを識別するための識別情報である。第 1 の識別情報は、具体的には、WAN 側に公開するネットワーク制御装置 101A の IP アドレス、および、ポート番号である。また、第 2 の識別情報は、ネットワーク制御装置 101A (の TCP / IP 通信処理部 302) への送信データを識別するための識別情報である。第 2 の識別情報は、具体的には、LAN 側に公開するネットワーク制御装置 101A の IP アドレス、および、ポート番号である。ホームルーターは、第 1 の識別情報 (WAN 側に公開する IP アドレス、ポート番号) の付されたデータを、インターネット 100 から (WAN 側から) 受信すると、そのデータがネットワーク制御装置 101宛てのデータであることを識別する。その場合、ホームルーターは、そのデータに、第 2 の識別情報 (LAN 側に公開する IP アドレス、ポート番号) を付して (宛先のアドレス、ポート番号を変更して) 、LAN 側に (ネットワーク制御装置 1 に) 送信する。

【 0 0 7 7 】

ネットワーク制御装置 101A (の TCP / IP 通信処理部 302) は、その第 2 の識別情報が付されたデータを受信すると、そのデータがネットワーク制御装置 101A (の TCP / IP 通信処理部 302) 宛てであることを識別する。

【 0 0 7 8 】

また、ネットワーク制御装置 101A は、インターネット 101 とは異なる媒体である記憶メディア 102 を介してネットワーク制御装置 101B に入力される第 1 の識別情報を、記憶メディア 102 に出力する。そして、ネットワーク制御装置 101A は、第 1 の識別情報が入力されたネットワーク制御装置 101B から送信され、ホームルーター (中継装置) により中継された送信データを、第 2 の識別情報により識別して受信する。

【 0 0 7 9 】

本実施形態では、UPnP による Internet Gateway Device のポート番号を設定した。しかしながら、その代わりに、Simple Traversal of UDP through NAT (STUN) 等によるホームルーターの NA

10

20

30

40

50

T越えの設定を行う処理でも良い。STUNを実行する為には、インターネット上に、グローバルIPアドレスを2つ持つSTUNサーバーが必要である。すなわち、STUNサーバーは、インターネット(通信媒体)100上の通信装置である。STUNサーバーは、2つのグローバルIPアドレスと2つのポート番号を使用する。また、ネットワーク制御装置101Aは、STUNサーバーに通信するためのSTUNクライアントを持つ(STUNクライアントとして動作する)。

【0080】

STUNクライアント(ネットワーク制御装置101A)とSTUNサーバー間で、STUNクライアントの1つのIPアドレスと1つのポート番号と、STUNサーバーの2つのグローバルIPアドレスと2つのポート番号を使用し、UDPを利用したテストメッセージの送受信を行う。このテストメッセージにより、NATの種類を判別することができ、Cone型のNATである場合には、STUNによるNAT越えによりネットワークの設定が可能であると判定する。NAT越えを実現する場合は、STUNクライアントとSTUNサーバー間でNATキャッシュを保持できるようにUDPによるメッセージの交換を定期的に行う。

【0081】

STUNクライアントはSTUNサーバーからホームルーターのWAN(ネットワーク制御装置101B)側に公開するIPアドレス、および、ポート番号を取得する。図1の103に位置するホームルーターのWAN側(インターネット100側)からアクセスする通信ノード(ネットワーク制御装置101B)が、STUNサーバーから取得したIPアドレス、および、ポート番号に対してUDPで通信を開始する。以上により、ホームルーターのNAT越えを実現することができる。

【0082】

すなわち、ネットワーク制御装置101Aは、送信装置であるネットワーク制御装置Bから送信された送信データを、伝送媒体であるインターネット100を介して受信する。また、ネットワーク制御装置101Aは、識別情報(WAN側に公開するネットワーク制御装置101AのIPアドレス、および、ポート番号)を、インターネット100上の通信装置であるSTUNサーバーから受信する。この識別情報は、ネットワーク制御装置101Bからネットワーク制御装置101A(のTCP/IP通信処理部302)へ送信された送信データを、ホームルーター(中継装置)が識別するための識別情報である。この識別情報は、具体的には、WAN側に公開するネットワーク制御装置101AのIPアドレス、および、ポート番号である。

【0083】

ホームルーター(中継装置)は、ネットワーク制御装置101Aをインターネット100に接続する。ホームルーターは、WAN側に公開するネットワーク制御装置101AのIPアドレス、および、ポート番号(識別情報)の付されたデータを受信すると、そのデータがネットワーク制御装置101A宛てであることを識別する。

【0084】

また、インターネット制御装置101Aは、記憶メディア102を介してネットワーク制御装置101Bに入力される識別情報(WAN側に公開するネットワーク制御装置101AのIPアドレス、および、ポート番号)を、記憶メディア102に出力する。記憶メディア102は、インターネット100とは異なる媒体である。そして、ネットワーク制御装置101Aは、識別情報が入力されたネットワーク制御装置101Bから送信され、ホームルーター(中継装置)により中継された送信データを受信する。

【0085】

なお、UPnPによるInternet Gateway Deviceのポート番号を設定する場合もSTUNの場合も、ホームルーターのWAN(ネットワーク制御装置101B)側のIPアドレスは指定できない。UPnPによるInternet Gateway Deviceのポート番号を設定する場合は、WAN側のポート番号が指定できるのに対して、STUNの場合は、WAN側のポート番号は指定できない。ネットワーク

10

20

30

40

50

制御装置 101A は、ホームルーターそのものへの設定は行わない。STUN を利用して、STUN サーバーから取得した、STUN サーバー間で作られたエントリのホームルーターの WAN 側の IP アドレス、および、ポート番号を記憶メディア 102 に保存する。

【0086】

ステップ S407において、論理ネットワークの接続受付の開始を通知し、処理を終了する。接続受付の開始情報を必要とするノード乃至処理部に対して通知を行う。通知先は、論理ネットワークの接続受付の開始情報を必要とするノードのユニキャストアドレス、論理ネットワークの接続受付の開始情報を広告するマルチキャストアドレスなどでもよい。この通知先は、例えば、ネットワーク制御装置 101A とともに論理ネットワークに接続されているネットワーク制御装置（不図示）である。

10

【0087】

また、ステップ S408において、検出した記憶メディア 102 から論理ネットワークの接続設定情報を読み出し、ステップ S409 に進む。この接続設定情報は、情報保持部 304 で保持される。

【0088】

ステップ S409において、読み出した論理ネットワークの接続設定情報が、対応するネットワーク制御装置で生成した論理ネットワークの接続設定情報であるかの判定を行う。対応するネットワーク制御装置とは、論理ネットワークの接続設定情報を生成したネットワーク制御装置に関連付けられたネットワーク制御装置である。論理ネットワークの接続設定情報を生成したネットワーク制御装置に関連付けられたネットワーク制御装置は、論理ネットワークの接続設定情報を生成したネットワーク制御装置そのものには限らない。つまり、論理ネットワークの接続設定情報を生成するネットワーク制御装置 101A と、論理ネットワークの接続設定情報を受け付けるネットワーク制御装置は、分離しても良い。これは、ネットワーク制御装置そのものが、機能を分割し、ネットワーク上に分散した形態であると見なすことも可能である。

20

【0089】

例えば、ネットワーク制御装置 101A が生成した接続設定情報には、ネットワーク制御装置 101C（不図示）のアドレス、パスワード等を入っているとする。論理ネットワークの接続を開始するネットワーク制御装置 101B は、論理ネットワークの接続設定情報をを利用して、論理ネットワークの接続を開始するので、ネットワーク制御装置 101C に論理ネットワークの接続の開始を要求する。

30

【0090】

ステップ S409において、ネットワーク制御装置 101C では、ステップ S409 から「いいえ」に進む。なお、ネットワーク制御装置 101A とネットワーク制御装置 101C が同一のデータベース等を参照する形態では、ネットワーク制御装置 101C は、ネットワーク制御装置 101A の生成を知り、「はい」に進む。

【0091】

マルチキャスト（乃至、エニーキャスト）を利用するときにも、接続設定情報を生成したネットワーク制御装置と、接続要求を受け付けるネットワーク制御装置が、異なることがある。すなわち、ある論理ネットワーク接続を受け付けるネットワーク制御装置群に対するマルチキャストを送信した場合、ある論理ネットワーク接続を受け付けるネットワーク制御装置群に接続要求が到達する。その場合、接続設定情報を生成したネットワーク制御装置と、接続要求を受け付けるネットワーク制御装置が、異なることがある。

40

【0092】

尚、接続設定情報に含まれるアドレス等の比較により、接続設定情報が、論理ネットワークの接続設定情報を生成したネットワーク制御装置に関連付けられた情報か否かの判定は行う事ができる。

【0093】

ステップ S409において、読み出された論理ネットワークの接続設定情報が対応するネットワーク制御装置で生成された論理ネットワークの制御情報であった場合、ステップ

50

S 4 1 0 に進む。ステップ S 4 0 9 において、読み出された論理ネットワークの接続設定情報が対応するネットワーク制御装置で生成された論理ネットワークの接続設定情報でなかった場合、ステップ S 4 1 5 に進む。

【 0 0 9 4 】

ステップ S 4 1 0 において、論理ネットワークの接続設定情報を削除するか判定する。ここで、論理ネットワークへの接続の受付を行うネットワーク制御装置において、制御部 3 0 1 に対する、ユーザーインターフェースや他のプログラムによって、接続設定情報の削除に関する指示が入力される。削除の指示がなければ、削除しない。ステップ S 4 1 0 において、論理ネットワークの接続設定情報を削除する場合、ステップ S 4 1 1 に進む。ステップ S 4 1 0 において、論理ネットワークの接続設定情報を削除しない場合、ステップ S 4 1 5 に進む。

【 0 0 9 5 】

ステップ S 4 1 1 において、論理ネットワークの接続設定情報に適合するネットワークの設定を削除し、ステップ S 4 1 2 に進む。このステップ S 4 1 1 で削除されるネットワークの設定は、ステップ S 4 0 6 の、論理ネットワークの接続の開始処理によって設定された、ネットワーク上に存在するホームルーターのポート番号の設定等である。すなわち、ステップ S 4 0 5 で出力した（接続設定）情報（第1の宛先情報）と、ステップ S 4 0 8 で入力した（接続設定）情報（第2の宛先情報）が一致する場合に、TCP / IP 通信処理部 3 0 2 による送信データの受信を制限する。以降、第1の宛先情報による、インターネット 1 0 0 上のネットワーク制御装置からネットワーク制御装置 1 0 1 A へのデータ送信は、ネットワーク制御装置 1 0 1 A (の TCP / IP 通信処理部 3 0 2) により、受信されない。

【 0 0 9 6 】

制御部 3 0 1 が、ステップ S 4 0 6 でホームルーターのポート番号の設定を行った場合には、ステップ S 4 0 6 では、UPnP による Internet Gateway Device のポート番号の設定を削除する。この削除は、UPnP による Internet Gateway Device に Delete Port Mapping により行う。なお、ステップ S 4 0 6 で、STUN 等によるホームルーターの NAT 越えの設定を行った場合、ステップ S 4 1 1 では、このホームルーターの NAT 越えの設定を行う処理を終了する。

【 0 0 9 7 】

すなわち、ステップ S 4 0 5 で出力した（接続設定）情報（第1の宛先情報）と、ステップ S 4 0 8 で入力した（接続設定）情報（第2の宛先情報）が一致する場合に、ホームルーターによるネットワーク制御装置 1 0 1 A (の TCP / IP 通信処理部 3 0 2) への送信データの転送を制限する。ホームルーターは、ネットワーク上の装置である。以降、第1の宛先情報による、インターネット 1 0 0 上のネットワーク制御装置からネットワーク制御装置 1 0 1 A へのデータ送信は、ホームルーターにより、ネットワーク制御装置 1 0 1 A には、転送されない。

【 0 0 9 8 】

ステップ S 4 1 2 において、論理ネットワークの接続設定情報を記憶メディア 1 0 2 から削除し（記憶メディア 1 0 2 上の接続設定情報（識別情報）を無効にし）、ステップ S 4 1 3 に進む。ステップ S 4 1 3 において、論理ネットワークの接続受付の終了処理を行い、ステップ S 4 0 3 で生成された対応する論理ネットワークの接続受付情報を情報保持部 3 0 4 から削除し、ステップ S 4 1 4 に進む。

【 0 0 9 9 】

ステップ S 4 1 4 において、論理ネットワークの接続受付の終了を通知し、処理を終了する。接続受付の終了情報を必要とするノード乃至処理部に対して通知を行う。通知先は、論理ネットワークの接続受付の終了情報を必要とするノードのユニキャストアドレス、論理ネットワークの接続受付の終了情報を広告するマルチキャストアドレスなどでもよい。この通知先は、例えば、論理ネットワークに接続されているネットワーク制御装置（不

10

20

30

40

50

図示)である。

【0100】

このように、ネットワーク制御装置101Aは、受信装置である。ネットワーク制御装置101Aは、送信装置であるネットワーク制御装置101Bに入力される第1の宛先情報を、記憶メディア102に出力し(ステップS405)、ネットワーク制御装置101Bから送信された送信データを受信する。そして、ネットワーク制御装置101Aは、記憶メディア102から第2の宛先情報を入力し(ステップS408)、第1の宛先情報と第2の宛先情報が一致する場合に(ステップS409)、インターネット100からのデータ受信を制限する(ステップS413)。

【0101】

また、ステップS415において、ステップS408で読み出した論理ネットワークの接続設定情報を用いて、論理ネットワークに接続するか判定する。ここでは、前記の論理ネットワークの接続設定情報に対応する論理ネットワークに接続していない場合、接続処理を行う。論理ネットワークの接続設定情報に対応する論理ネットワークに既に接続している場合は、接続を行わない。この判断は、論理ネットワークを受け付ける接続設定情報の比較((接続設定情報に含まれるネットワーク制御装置101Aの)アドレスの比較)により、接続済みの論理ネットワークと同じであるかの判断を行う。また、制御部301に対する、ユーザーインターフェースや他のプログラムによって、接続設定情報の接続に関する指示を入力することにより、論理ネットワークに接続するか否かの決定してもよい。

10

20

【0102】

ステップS415において、ステップS408で読み出した論理ネットワークの接続設定情報を用いて、論理ネットワークに接続する場合、ステップS416に進む。ステップS415において、論理ネットワークの接続設定情報を用いて、論理ネットワークに接続しない場合、処理を終了する。

【0103】

ステップS416において、ステップS408で読み出した論理ネットワークの接続設定情報を用いて、論理ネットワークへの接続を開始し、ステップS417に進む。論理ネットワークの接続設定情報には、論理ネットワークへの接続許可を行うノード(上述の例では、ネットワーク制御装置101A)のIPアドレス、ポート番号、プロトコル、認証方式、パスワードなどの情報が含まれる。すなわち、接続設定情報は、接続許可を送信する場合の接続許可の宛先を示す宛先情報である。

30

【0104】

ステップS417において、論理ネットワークへの接続の開始を通知し、処理を終了する。この通知は、論理ネットワークの接続の開始情報を必要とするノード乃至処理部に対して行う。通知先は、既に論理ネットワークに接続しているノード(ネットワーク制御装置など)、論理ネットワークの接続の開始情報を必要とするノードのユニキャストアドレス、論理ネットワークの接続の開始情報を広告するマルチキャストアドレスなどでもよい。ここで接続開始の通知は、ネットワーク制御装置101Bが接続しているインターネット100に接続の開始情報を広告する。

40

【0105】

すなわち、ネットワーク制御装置101Bは、送信装置であって、ネットワーク制御装置101Aと同様に、他の送信装置に入力される第1の宛先情報を記憶メディア102に出力する(ステップS405)。また、ネットワーク制御装置101Bは、記憶メディア102から第2の宛先情報を入力する(ステップS408)。そして、ネットワーク制御装置101Bは、第1の宛先情報と第2の宛先情報が一致しない場合に(ステップS409)、第2の宛先情報を付与した論理ネットワークへの参加要求(送信データ)を送信する(ステップS417)。ここで、第1の宛先情報と第2の宛先情報が一致しないとは、ステップS408でネットワーク制御装置に入力された宛先情報が、その宛先情報が入力されたネットワーク制御装置自身が出力(ステップS405)した宛先情報ではないこと

50

を意味する。

【0106】

この論理ネットワークに接続されているネットワーク制御装置101A及び不図示のネットワーク制御装置は、論理ネットワークへの接続開始の通知をネットワーク制御装置101Bから受け付けると、ネットワーク制御装置101BのIPアドレス（ユニキャストアドレス）を認識する。ステップS406で接続受付を開始してからステップS413で接続受付を終了するまでは、この論理ネットワークへの接続開始の通知を受け付けることが可能である。

【0107】

本実施形態の記憶メディアとの接続の切断検出時のシーケンスについて、図5のフローチャートを参照して説明する。図5は、HDD209又はFDD210に記憶されたコンピュータプログラムの一部を表わす。コンピュータであるCPU201は、このプログラムを、HDD209又はFDD210から読み出して、図5のフローチャートに対応する動作を行う。HDD209又はFDD210は、このプログラムを、CPU201が読み出すことができるよう記憶した記憶媒体である。

10

【0108】

ステップS501において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続が接続中であるかの判定を行う。ステップS501において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続が接続中である場合、ステップS502に進む。ステップS501において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続が接続中でない場合、ステップS506に進む。

20

【0109】

ステップS502において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続を終了するか判定する。ここで、記憶メディア102の接続中に、ユーザーインターフェースや他のプログラム等により、論理ネットワーク接続の継続を設定された場合には、接続を継続する。そうでなければ、接続を終了する。また、記憶メディア102の切断後に、接続設定情報の切断に関する指示を入力することにより、接続設定情報を切断してもよい。この判定を削除し、無条件に、接続を終了するようにしても良い。ステップS502において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続を終了する場合、ステップS503に進む。ステップS502において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続を継続する場合、処理を終了する。

30

【0110】

ステップS503において、切断を検出した記憶メディア102に関連付けられた論理ネットワークとの接続を切断し、ステップS504に進む。

【0111】

ステップS504において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続の切断通知を行い、ステップS505に進む。論理ネットワークの接続の切断情報を必要とするノード乃至処理部に対して通知を行う。通知先は、論理ネットワークに接続しているノード（ネットワーク制御装置101Aなど）、論理ネットワークの接続の切断情報を必要とするノードのユニキャストアドレス、論理ネットワークの接続の切断情報を広告するマルチキャストアドレスなどでもよい。

40

【0112】

ステップS505において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続設定情報を情報保持部304から削除し、処理を終了する。ネットワーク制御装置101Bは、ステップS408で読み出した接続設定情報を削除する。

【0113】

ステップS506において、切断を検出した記憶メディア102に関連付けられた論理ネットワークの接続設定情報が情報保持部304に存在するかの判定を行う。エラーやユ

50

ーザーインターフェースや他のプログラムから論理ネットワークの接続の切断がなされた場合、論理ネットワークの接続設定情報が削除されているとは限らない。したがって、論理ネットワークの接続設定情報が削除されていない場合には、論理ネットワークの接続設定情報を削除する。一方、何らかの手段により、論理ネットワークの接続設定情報の削除がなされていた場合、ステップ S 5 0 6 において、論理ネットワークの設定情報は存在しない。

【 0 1 1 4 】

ステップ S 5 0 6 において、切断を検出した記憶メディア 1 0 2 に関連付けられた論理ネットワークの接続設定情報が情報保持部 3 0 4 に存在する場合、ステップ S 5 0 5 に進む。ステップ S 5 0 6 において、接続を検出した記憶メディア 1 0 2 に関連付けられた論理ネットワークの接続設定情報が制御部に存在しない場合、処理を終了する。

10

【 0 1 1 5 】

本実施形態の記憶メディア 1 0 2 に格納される情報について、図 6 を参照して説明する。

図 6 において、記憶メディア 1 0 2 に 2 つの論理ネットワークの接続設定情報が格納されている。記憶メディアの接続設定情報の格納個数を限定するものではなく、0 を含む任意の個数の接続設定情報を格納してもよい。

【 0 1 1 6 】

図 6 において、接続先情報は、論理ネットワークが何であるかを示す情報が格納される。本実施例では、家族と様々なサービスを共有するための論理ネットワークをファミリー、会社と様々なサービスを共有する論理ネットワークをオフィスとする。

20

【 0 1 1 7 】

図 6 において、IP アドレスは、論理ネットワークの接続を許可する接続先（ネットワーク制御装置 1 0 1 A ）の IP アドレスである。本実施形態では、IP アドレスは、IP v 4 アドレス、IP v 6 アドレスを格納しているが、これに限らず、他の IP アドレスの形式を格納してもよい。

【 0 1 1 8 】

図 6 において、ポート番号は、論理ネットワークの接続を許可する接続先（ネットワーク制御装置 1 0 1 A ）のポート番号である。

【 0 1 1 9 】

図 6 において、プロトコルは、論理ネットワークの接続を許可する接続先に通信を行う時に用いる、トランSPORTプロトコルである。トランSPORTプロトコルは、TCP、UDP を格納可能であり、これに限らず、他のトランSPORTプロトコル（例えば、Stream Control Transmission Protocol (SCTP) ）を格納してもよい。

30

【 0 1 2 0 】

図 6 において、認証タイプは、論理ネットワークの接続を許可する接続先に通信を行う時に用いる、認証方法・暗号化方法である。共通鍵を用いる認証方法・暗号化方法、乃至、共通鍵を用いる認証方法・暗号化方法を格納しており、これに限らず、他の認証方法・暗号化方法およびアルゴリズムを格納してもよい。

40

【 0 1 2 1 】

図 6 において、共通鍵は、論理ネットワークの接続を許可する接続先との認証・暗号化に用いる 256 ビットの共通鍵である。共通鍵は、これに限らず、任意長の共通鍵を格納してもよい。

【 0 1 2 2 】

図 6 において、公開鍵は、論理ネットワークの接続を許可する接続先との認証・暗号化に用いる、論理ネットワークの接続を許可する接続先の 4096 ビットの公開鍵である。公開鍵は、これに限らず、任意長の公開鍵を格納してもよい。

【 0 1 2 3 】

図 6 において、ライフタイムは、接続パラメーターの有効時間である。ライフタイムが

50

ある間は、論理ネットワークの接続を許可する接続先に接続を行う事が可能である。本実施形態において、ライフタイムは一週間、一ヶ月であるが、これに限らず、任意のライフタイム、乃至、無限長のライフタイムを格納してもよい。

【0124】

図6に追加する形で、論理ネットワークのパラメーター（論理ネットワーク上のアドレス、乃至、ID、論理ネットワーク上の経路情報等）を格納してもよい。

【0125】

本実施形態では、接続受付情報は、接続設定情報に対応した認証情報を持つ。接続受付情報には、IPアドレス、ポート番号、ライフタイム、論理ネットワークのパラメーター等を格納してもよい。この接続受付情報に含まれる認証情報は、図6の認証タイプ、共通鍵、公開鍵である。接続設定情報と接続受付情報の認証情報は対になっている。

10

【0126】

本実施形態では、論理ネットワークへの接続に必要な接続設定情報を簡単に設定でき、論理ネットワークへの接続を開始する時の煩雑な処理を低減することができる。

【0127】

記憶メディア102の接続により、ネットワークの設定の生成および削除、論理ネットワークへの接続および切断、を簡単に行うことができる。ユーザーインターフェースの貧弱な機器（例えば、デジタルカメラ、プリンタ）に適用することで、煩雑なパラメーターの設定のフェーズを回避することができ、ユーザーは簡単に利用することができる。

【0128】

20

<実施形態2>

本実施形態のネットワークシステムの構成について、図8を参照して説明する。実施形態2において、基本的な構成は実施形態1と共通であり、本実施形態の説明においては、実施形態1と異なる部分について説明する。

【0129】

801は、記憶メディア102の情報の一部を管理する情報格納サーバーである。前述した実施形態1の記憶メディア102の一部を情報格納サーバー801に格納することによって、記憶メディア201に格納する情報量を軽減することができる。本実施形態では、情報格納サーバー801は1台であるが、これに限らず、情報格納サーバー801はネットワークを介して複数に分散していくてもよい（例えば、分散ハッシュテーブルを用いたピア・ツー・ピア接続）。

30

【0130】

図9において、制御部301は、記憶メディア102の情報を用いて、情報格納サーバー801とTCP/IP通信部302を通じて、通信を行う。情報格納サーバー801の指定方法は、情報格納サーバー801を直接指定するユニキャスト、情報格納サーバー群を指定するマルチキャスト、情報格納サーバー801用のエニーキャストを用いることができる。

【0131】

記憶メディア102と情報格納サーバー801を予め関連付けておくことで、記憶メディア102に記憶された情報から情報格納サーバー801へアクセスすることができる。すなわち、記憶メディア102に、情報格納サーバーのアドレスが記憶されている。サーバーに直接アクセスする場合、このアドレスは、IPアドレスである。

40

【0132】

本形態では、図4のステップS405において、生成した論理ネットワークの接続設定情報の一部、パラメーターのIDを記憶メディア102に格納する。情報格納サーバーのアドレスは、あらかじめ記憶メディアに格納されている。記憶メディア102に格納される情報については、後述する。また、生成した論理ネットワークの接続設定情報の一部と、前記IDを情報格納サーバー801に格納する。情報格納サーバー801に格納される情報については、後述する。

【0133】

50

また、ステップS408において、記憶メディア102に格納されている論理ネットワークの接続設定情報の一部、情報格納サーバー801のアドレス、パラメーターIDを読み出す。記憶メディア102に関連付けられた情報格納サーバー801に、前記IDを送信する。情報格納サーバー801は、前記IDに対応するパラメーターを検索し、論理ネットワークの接続設定情報の一部を返信する。ステップS416では、情報格納サーバー801から返信された接続設定情報を用いて接続を開始する。

【0134】

ステップS412において、論理ネットワークの接続設定情報の一部、IDを記憶メディア102から削除し(記憶メディア102の識別情報を無効にし)、前記IDに対応する論理ネットワークの接続設定情報の一部を情報格納サーバー801から削除する。すなわち、TCP/IP通信処理部302によりインターネット(ネットワーク)801上の装置である情報格納サーバー801から接続設定情報(第2の宛先情報)を受信する(ステップS408)。そして、制御部301は、その情報格納サーバー801から受信した接続設定情報(第2の宛先情報)が、ステップS405で出力した接続設定情報(第1の宛先情報)と一致する場合に、情報格納サーバー801に記憶された接続設定情報を無効にする(ステップS412)。また、制御部301は、情報格納サーバー801から受信した接続設定情報(第2の宛先情報)が、ステップS405で出力した接続設定情報(第1の宛先情報)と一致する場合に、TCP/IP通信処理部302による送信データの受信を制限する(ステップS413)。

【0135】

また、本実施形態においても、制御部301が、ステップS406でホームルーターのポート番号の設定を行った場合には、ステップS406では、UPnPによるInternet Gateway Deviceのポート番号の設定を削除する。この削除は、UPnPによるInternet Gateway DeviceにDeletePort Mappingにより行う。なお、ステップS406で、STUN等によるホームルーターのNAT越えの設定を行った場合、ステップS411では、このホームルーターのNAT越えの設定を行う処理を終了する。すなわち、ステップS405で出力した情報(第1の宛先情報)と、ステップS408で受信した情報(第2の宛先情報)が一致する場合に、ホームルーターによるネットワーク制御装置101A(のTCP/IP通信処理部302)への送信データの転送を制限する。ホームルーターは、ネットワーク上の装置である。

【0136】

また、本実施形態においても、ネットワーク制御装置101Bは、送信装置であって、他の送信装置に入力される第1の宛先情報を記憶メディア102に出力する(ステップS405)。また、ネットワーク制御装置101Bは、情報格納サーバー801から第2の宛先情報を受信する(ステップS408)。そして、ネットワーク制御装置101Bは、第1の宛先情報と第2の宛先情報が一致しない場合に(ステップS409)、第2の宛先情報を付与した論理ネットワークへの参加要求(送信データ)を送信する(ステップS417)。

【0137】

本実施形態の記憶メディア102に格納される情報について、図10を参照して説明する。

図10において、情報格納サーバー801は、記憶メディア102に関連付けられた情報格納サーバーのIPアドレスを示す。

図10において、IDは、パラメーターの識別子であり、情報格納サーバー801から情報を引き出す際の識別子として利用される。

図10において、接続先情報は、論理ネットワークが何であるかを示す情報が格納される。

【0138】

本実施形態において、記憶メディア102の接続設定情報の格納個数を限定するもので

10

20

30

40

50

はなく、0を含む任意の個数の接続設定情報を格納してもよい。

【0139】

本実施形態の情報格納サーバー801に格納される情報について、図11を参照して説明する。本実施形態における、一例として、図11の情報格納サーバー801に格納される情報を保持する情報格納サーバー801のIPアドレスは150.150.150.1とする。図10に示した記憶メディア102に格納される情報と図11に示した情報格納サーバー801に格納される情報には関連がある。

【0140】

図11において、IDは、パラメーターの識別子であり、情報格納サーバー801から情報を引き出す際の識別子として利用される。図11のIDは、図10のIDと対応する。

10

【0141】

図11において、IPアドレス、ポート番号、プロトコル、認証タイプ、共通鍵、公開鍵、ライフタイムの定義は、図6と共通である。

【0142】

<実施形態3>

本実施形態のネットワークシステムの構成について、図8を参照して説明する。実施形態3において、基本的な構成は実施形態2と共通であり、本実施形態の説明においては、実施形態2と異なる部分について説明する。

【0143】

20

ネットワーク制御装置101Aと情報格納サーバー801を予め関連付けておく事で、記憶メディア102と情報格納サーバー801を関連付けさせることができる。

【0144】

図9において、情報保持部304が、生成する接続設定情報に関連付けられた情報格納サーバー801のアドレスを保持し、制御部301が、前記関連付けられた情報格納サーバー801のアドレスを記憶メディア102に格納する。このように構成することで、記憶メディア102と情報格納サーバー801を関連付けることができる。

【0145】

本形態では、図4のステップS405において、論理ネットワークの接続設定情報の一部、情報格納サーバー801のアドレス、パラメーターのID(図10)を記憶メディア102に格納する。また、論理ネットワークの接続設定情報の一部と、前記ID(図11)を情報格納サーバー801に格納する。

30

【0146】

また、ステップS408において、記憶メディア102に格納されている論理ネットワークの接続設定情報の一部、情報格納サーバー801のアドレス、IDを読み出す。その後、情報格納サーバー801に前記IDを送信し、情報格納サーバー801が前記IDによる検索を行い、論理ネットワークの接続設定情報の一部を返信する。ステップS416では、情報格納サーバー801から返信された接続設定情報を用いて接続を開始する。

【0147】

ステップS412において、記憶メディア102に格納されている論理ネットワークの接続設定情報の一部、情報格納サーバー801のアドレス、IDを削除する。また、前記IDに対応して情報格納サーバー801に格納されている論理ネットワークの接続設定情報の一部を削除する。すなわち、情報格納サーバー801から受信された接続設定情報(第2の宛先情報)が、ステップS405で出力した接続設定情報(第1の宛先情報)と一致する場合に、情報格納サーバー801に記憶された接続設定情報(第2の識別情報)を無効にする。情報格納サーバー801は、インターネット(ネットワーク)100上の装置である。また、制御部301は、その情報格納サーバー801から受信した接続設定情報(第2の宛先情報)が、ステップS405で出力した接続設定情報(第1の宛先情報)と一致する場合に、TCP/IP通信処理部302による送信データの受信を制限する(ステップS413)。

40

50

【0148】

また、本実施形態においても、制御部301が、ステップS406でホームルーターのポート番号の設定を行った場合には、ステップS406では、UPnPによるInternet Gateway Deviceのポート番号の設定を削除する。この削除は、UPnPによるInternet Gateway DeviceにDeletePortMappingにより行う。なお、ステップS406で、STUN等によるホームルーターのNAT越えの設定を行った場合、ステップS411では、このホームルーターのNAT越えの設定を行う処理を終了する。すなわち、ステップS405で出力した情報（第1の宛先情報）と、ステップS408で受信した情報（第2の宛先情報）が一致する場合に、ネットワーク上の装置であるホームルーターによるネットワーク制御装置101A（のTCP/IP通信処理部302）への送信データの転送を制限する。

【0149】

また、本実施形態においても、ネットワーク制御装置101Bは、送信装置であって、他の送信装置に入力される第1の宛先情報を記憶メディア102に出力する（ステップS405）。また、ネットワーク制御装置101Bは、情報格納サーバー801から第2の宛先情報を受信する（ステップS408）。そして、ネットワーク制御装置101Bは、第1の宛先情報と第2の宛先情報が一致しない場合に（ステップS409）、第2の宛先情報を付与した論理ネットワークへの参加要求（送信データ）を送信する（ステップS417）。

【0150】

<実施形態4>

以上の形態では、ネットワーク制御装置101Aから情報を記憶メディア101に出力し、その記憶メディア101からネットワーク制御装置101Bに情報を入力した。しかしながら、ネットワーク制御装置101Aから101Bへの情報を移送する仲介する媒体は、記憶メディアには、限らない。例えば、ネットワーク制御装置101Aから情報を紙などに記録し、ネットワーク制御装置101Bが、紙などに記録された情報を、光学的に読み取って、その情報を認識しても良い。紙などに記録する場合、バーコードなどの符号化された形式で、情報を記録しても良い。

【0151】

また、ネットワーク制御装置101Bが携帯型の装置の場合、記憶メディア101を介さずに、直接、近距離無線通信により、ネットワーク制御装置101Aから101Bに、情報を転送することもできる。このようにしても、ネットワーク制御装置101Bをネットワーク制御装置101Aの遠隔に持ち出す場合には有効である。

【0152】

本発明の目的は前述した実施例の機能を実現するソフトウェアのプログラムコードを記録した記録媒体を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはCPUまたはMPU）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成される。この場合、記憶媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することとなり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。

【0153】

プログラムコードを供給するための記憶媒体としては、例えば、フレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、CD-R、不揮発性のメモリカード、ROM、DVDなどを用いることができる。

【0154】

また、本発明は、コンピュータが読み出したプログラムコードを実行することにより、前述した実施例の機能が実現される形態には限られない。すなわち、本発明は、そのプログラムコードの指示に基づき、コンピュータ上で稼動しているOperating System(OS)などが実際の処理の一部または全部を行い、その処理によって前述した実施例の機能が実現される場合も含まれる。

10

20

30

40

50

【0155】

さらに、記憶媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書きこまれた後、そのプログラムコードの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるCPUなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれる。

【図面の簡単な説明】

【0156】

【図1】実施形態1におけるネットワークシステム構成図である。

【図2】本発明の一実施形態に係る101をPC(パーソナルコンピュータ)を使用して 10 実現した場合のシステムブロック図である。

【図3】実施形態1における内部モジュール構成図である。

【図4】記憶メディアの接続を検出した際のシーケンスを示したフローチャートである。

【図5】記憶メディアの切断を検出した際のシーケンスを示したフローチャートである。

【図6】記憶メディアに格納される論理ネットワークの接続設定情報である。

【図7】ある状態に対応したネットワーク制御装置および記憶メディアの格納情報である

。

【図8】実施形態2におけるネットワークシステム構成図である。

【図9】実施形態2におけるモジュール構成図である。

【図10】記憶メディアに格納される情報である。 20

【図11】情報格納サーバーに格納される情報である。

【符号の説明】

【0157】

100 インターネット

101A、B ネットワーク制御装置

102 記憶メディア

301 制御部

302 TCP/IP 通信処理部

303 NFC 通信処理部

304 情報保持部

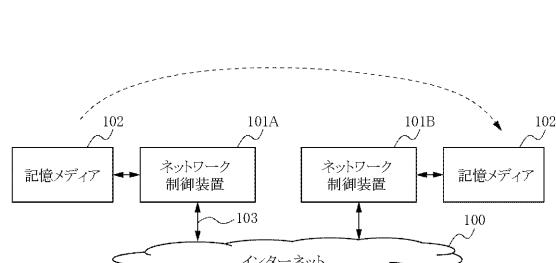
305 ネットワーク制御部

801 情報格納サーバー

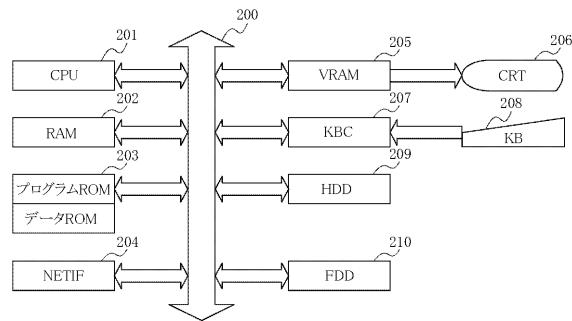
20

30

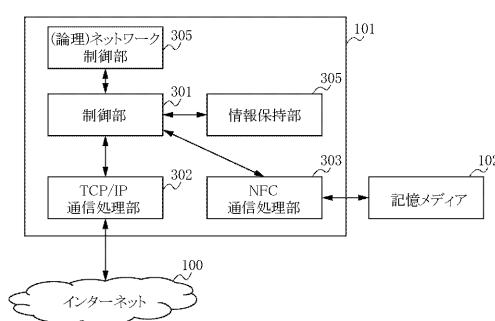
【図1】



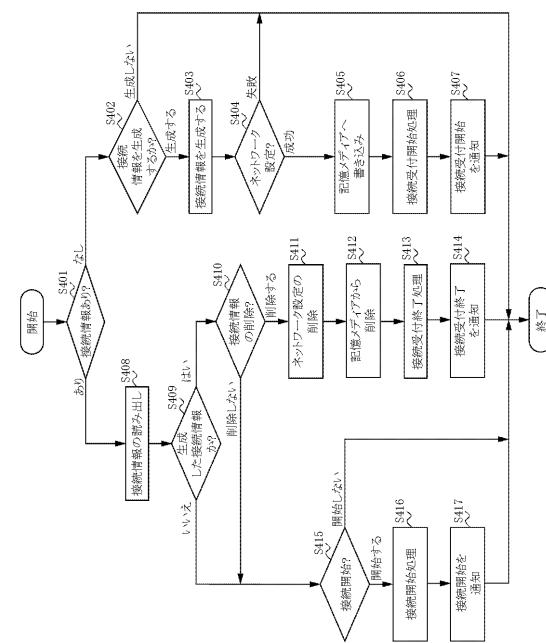
【図2】



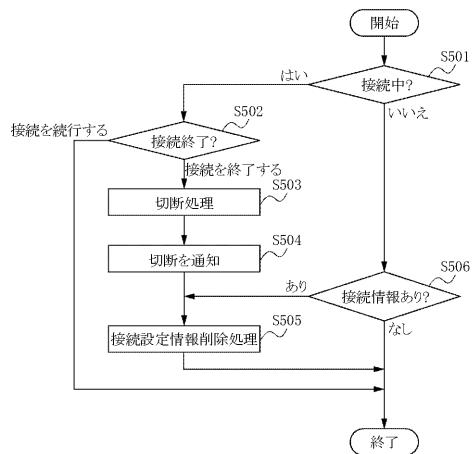
【図3】



【図4】



【図5】



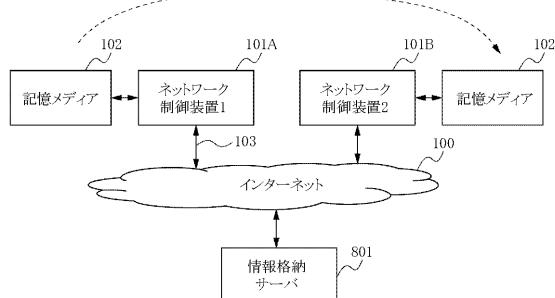
【図6】

	パラメータ1	パラメータ2
接続先情報	ファミリー	オフィス
IPアドレス	2001:200:1	200.100.10.1
ポート番号	1000	2000
プロトコル	TCP	UDP
認証タイプ	共通鍵	公開鍵
共通鍵	256bit	256bit
公開鍵	4096bit	4096bit
ライフタイム	一週間	一ヶ月

【図7】

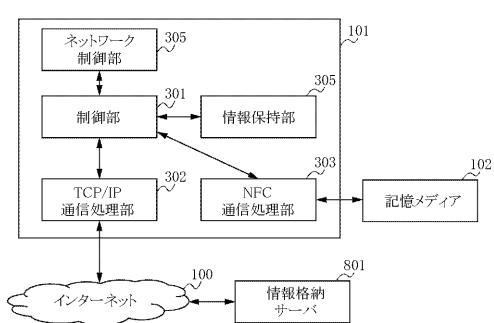
状態	ネットワーク制御装置101A	ネットワーク制御装置101B	記憶メディア
(1)	接続受付情報	なし	接続設定情報
(2)	接続受付情報	接続設定情報	接続設定情報
(3)	接続受付情報	なし	接続設定情報
(4)	なし	なし	なし

【図8】



【図9】

【図10】



	パラメータ1	パラメータ2
情報格納サーバ	150.150.150.1	100.100.100.1
ID	1000	2000
接続先情報	アミリー	オフィス

【図11】

	パラメータ1	パラメータ2
ID	1000	3000
IPアドレス	2001:200::1	200.100.10.1
ポート番号	1000	2000
プロトコル	TCP	UDP
認証タイプ	共通鍵	公開鍵
共通鍵	256bit	256bit
公開鍵	4096bit	4096bit
ライフタイム	一週間	一ヶ月

フロントページの続き

(56)参考文献 特開2005-175865(JP,A)
特開2006-67174(JP,A)
特開2004-40738(JP,A)
特開2003-283524(JP,A)
特開2002-77274(JP,A)

(58)調査した分野(Int.Cl., DB名)

H04L 12/66
H04L 12/56
H04L 12/46
H04L 12/28