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

特許第5687388号
(P5687388)

(45)発行日　平成27年3月18日(2015.3.18)　(24)登録日　平成27年1月30日(2015.1.30)

(51)Int.Cl.　F I
H04L 12/28 (2006.01)　H04L 12/28 100H
H04L 12/70 (2013.01)　H04L 12/70 D
H04L 12/70 A

請求項の数 9　(全 35 頁)

(21)出願番号　特願2014-511920 (P2014-511920)
(86)(22)出願日　平成24年5月22日(2012.5.22)
(65)公表番号　特表2014-522590 (P2014-522590A)
(43)公表日　平成26年9月4日(2014.9.4)
(86)国際出願番号　PCT/FI2012/050484
(87)国際公開番号　WO2012/160257
(87)国際公開日　平成24年11月29日(2012.11.29)
審査請求日　平成26年8月6日(2014.8.6)
(31)優先権主張番号　20115512
(32)優先日　平成23年5月24日(2011.5.24)
(33)優先権主張国　フィンランド(FI)

早期審査対象出願

(73)特許権者　513211571
トシボックス・オイ
フィンランド・ＦＩ－９０５９０・オウル・エレクトロニーカティエ・１０
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉
(72)発明者　ヴェイコ・イリマルティモ
フィンランド・９０４２０・オウル・パロケルイエンティ・４

最終頁に続く

(54)【発明の名称】建物の遠隔制御を実施するためのデバイス構成

(57)【特許請求の範囲】
【請求項１】
建物内のアクチュエータのためのホームコントロールネットワークキー(42、42b)であって、
- ネットワークインターフェース(3、4)のための入力/出力手段(424、425、426、427)を含むネットワークインターフェース要素と、
- プロセッサ(422)と、
- コンピュータプログラムコードを含むメモリ(423)とを含み、
- 前記プロセッサ、前記メモリ、および前記メモリに記憶されたコンピュータプログラムコードが、
- 前記ホームコントロールネットワークキー(42、42b)からインターネット(2)へのネットワーク経路を判定し、
- 前記判定されたネットワーク経路を、ホームコントロールネットワークキーの前記メモリ(423)と、ホームコントロールネットワークサーバ(21)のメモリ(213)との両方に記憶するように構成される、ホームコントロールネットワークキー(42、42b)において、
前記プロセッサ、前記メモリ、および前記メモリに記憶されたコンピュータプログラムコードが、さらに、
- 前記ホームコントロールネットワークキー(42、42b)および一意のネットワーク端末のペア(61)が前記ホームコントロールネットワークキー(42、42b)および前記一意のネットワーク端末のペア(61)のUSBポート(426、627)によって1つに接続されるときに、前記ホー

ムコントロールネットワークキーだけがデータ転送接続を確立することを許される一意の端末デバイスであるホームコントロールネットワークキーの一意のネットワーク端末のペア(61)によって送信された一意のデバイス識別コードを受信するか、または前記ホームコントロールネットワークキー自体のデバイス識別コードをホームコントロールネットワークキーの一意のネットワーク端末のペア(61)に送信し、

- 前記ホームコントロールネットワークキー(42、42b)の前記一意のネットワーク端末のペア(61)へのエンドツーエンドのデータ転送接続を確立するための前記ホームコントロールネットワークキー(42、42b)の前記一意のネットワーク端末のペア(61)のネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)に要求し、
- 前記ホームコントロールネットワークキー(42、42b)の前記一意のネットワーク端末デバイスのペア(61)の前記ネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)から受信し、
- 前記受信されたネットワーク経路情報の助けを借りて、前記ホームコントロールネットワークキー(42、42b)の前記一意のネットワーク端末のペア(61)とともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワーク(55)を確立するように構成され、前記仮想プライベートネットワーク(55)には前記ホームコントロールネットワークサーバ(21)が属さないことを特徴とする、ホームコントロールネットワークキー(42、42b)。

【請求項２】

ホームコントロールネットワークキーの機能を実装するコンピュータプログラムを、前記ホームコントロールネットワークキー(42b)のメモリ(423)から、前記インターネットに接続されたデータ処理デバイス(41c)にインストールするように構成され、前記データ処理デバイス(41c)が、インストールされるコンピュータプログラムによって前記ホームコントロールネットワークキー(42b)の機能をシミュレートするように構成されることを特徴とする請求項1に記載のホームコントロールネットワークキー。

【請求項３】

ホームコントロールネットワークキーのシミュレーションを開始するために利用されるパスワードも前記データ処理デバイス(41c)にインストールするように構成されることを特徴とする請求項2に記載のホームコントロールネットワークキー。

【請求項４】

建物内のアクチュエータのためのホームコントロールネットワークデバイス(61)であって、

- ネットワークインターフェース(5)および遠隔制御されるべきデバイス(62～65)の両方のための入力/出力手段(624、625、626、627)を含むネットワークインターフェース要素と、
- 少なくとも1つのプロセッサ(622)と、
- コンピュータプログラムコードを含むメモリ(623)とを含み、

前記プロセッサ、前記メモリ、および前記メモリに記憶されたコンピュータプログラムコードが、

- 前記ホームコントロールネットワークデバイス(61)からインターネット(2)へのネットワーク経路を判定し、
- 前記判定されたネットワーク経路を、ホームコントロールネットワークデバイスの前記メモリ(623)と、ホームコントロールネットワークサーバ(21)のメモリ(213)との両方に記憶するように構成される、ホームコントロールネットワークデバイス(61)において、

前記プロセッサ、前記メモリ、および前記メモリに記憶されたコンピュータプログラムコードが、さらに、

- 前記ホームコントロールネットワークデバイス(61)およびネットワーク端末のペア(42、42b)が前記ホームコントロールネットワークデバイス(61)および前記ネットワーク端末のペア(42、42b)のUSBポート(426、627)によって1つに接続されるときに、前記ホームコ

ントロールネットワークデバイスだけがデータ転送接続を確立することを許される一意の端末デバイスであるホームコントロールネットワークデバイス(61)の一意のネットワーク端末のペア(42、42b)によって送信された一意のデバイス識別コードを受信するか、または前記ホームコントロールネットワークデバイス(61)自体のデバイス識別コードをホームコントロールネットワークデバイス(61)の一意のネットワーク端末のペア(42、42b)に送信し、

- 前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末のペア(42、42b)へのエンドツーエンドのデータ転送接続を確立するための前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末のペア(42、42b)のネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)に要求し、
- 前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末デバイスのペア(42、42b)の前記ネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)から受信し、
- 前記受信されたネットワーク経路情報の助けを借りて、前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末のペア(42、42b)とともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワーク(55)を確立するように構成され、前記仮想プライベートネットワーク(55)には前記ホームコントロールネットワークサーバ(21)が属さないことを特徴とする、ホームコントロールネットワークデバイス(61)。

【請求項５】

OSIモデルのデータリンク層(レイヤ2)かまたはネットワーク層(レイヤ3)かのどちらかで前記仮想プライベートネットワーク(55)を形成するように構成されることを特徴とする請求項4に記載のホームコントロールネットワークデバイス。

【請求項６】

ホームコントロールネットワークキーの機能を提供するための、コンピュータ可読ストレージ手段に記憶されたコンピュータプログラムコード手段を含むコンピュータプログラムであって、

- 前記ホームコントロールネットワークキー(42、42b)からインターネット(2)へのネットワーク経路を判定するためのコード手段と、
- 判定されたネットワーク経路を、前記ホームコントロールネットワークキーのメモリ(423)と、ホームコントロールネットワークサーバ(21)のメモリ(213)との両方に記憶するためのコード手段とを含み、

前記コンピュータプログラムが、さらに、

- ホームコントロールネットワークキー(42、42b)およびホームコントロールネットワークデバイス(61)のペアが前記ホームコントロールネットワークキー(42、42b)および前記ホームコントロールネットワークデバイス(61)のペアのUSBポート(426、627)によって１つに接続されるときに、前記ホームコントロールネットワークキーだけがデータ転送接続を確立することを許される一意の端末デバイスである一意のネットワーク端末のペア(61)によって送信された一意のデバイス識別コードを受信するか、または前記ホームコントロールネットワークキー(42、42b)自体のデバイス識別コードを一意のネットワーク端末のペア(61)に送信するためのコード手段と、
- 前記一意のネットワーク端末のペア(61)へのエンドツーエンドのデータ転送接続を確立するための前記一意のネットワーク端末のペア(61)のネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)に要求するためのコード手段と、
- 前記一意のネットワーク端末のペア(61)の前記ネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)から受信するためのコード手段と、
- 受信されたネットワーク経路情報を用いて、前記一意のネットワーク端末のペア(61)とともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワーク(55)を確立するためのコード手段とを含み、前記仮想プライベートネットワーク(55)には前記ホームコントロールネットワークサーバ(21)が属さないことを特徴とする、コンピュータプ

ログラム。
【請求項７】
前記ホームコントロールネットワークキー(42b)の機能がデータ処理デバイス(41c)によってシミュレートされ得るように、前記ホームコントロールネットワークキーの機能を実装するコンピュータプログラムを、前記ホームコントロールネットワークキー(42b)の前記メモリ(423)から、前記インターネットに接続された前記データ処理デバイス(41c)にインストールするように構成されたコード手段をさらに含むことを特徴とする請求項6に記載のコンピュータプログラム。
【請求項８】
ホームコントロールネットワークキーのシミュレーションを開始するために利用されるパスワードを前記ホームコントロールネットワークキー(42b)から前記データ処理デバイス(41c)にインストールするように構成されるコード手段をさらに含むことを特徴とする請求項7に記載のコンピュータプログラム。
【請求項９】
ホームコントロールネットワークデバイスの機能を提供するための、コンピュータ可読ストレージ手段に記憶されたコンピュータプログラムコード手段を含むコンピュータプログラムであって、
- 前記ホームコントロールネットワークデバイス(61)からインターネット(2)へのネットワーク経路を判定するためのコード手段と、
- 判定されたネットワーク経路を、前記ホームコントロールネットワークデバイスのメモリ(623)と、ホームコントロールネットワークサーバ(21)のメモリ(213)との両方に記憶するためのコード手段とを含み、
前記コンピュータプログラムが、さらに、
- 前記ホームコントロールネットワークデバイス(61)およびネットワーク端末のペア(42、42b)が前記ホームコントロールネットワークデバイス(61)および前記ネットワーク端末のペア(42、42b)のUSBポート(426、627)によって１つに接続されるときに、前記ホームコントロールネットワークデバイスだけがデータ転送接続を確立することを許される一意の端末デバイスであるホームコントロールネットワークデバイス(61)の一意のネットワーク端末のペア(42、42b)によって送信された一意のデバイス識別コードを受信するか、または前記ホームコントロールネットワークデバイス(61)自体のデバイス識別コードをホームコントロールネットワークデバイス(61)の一意のネットワーク端末のペア(42、42b)に送信するためのコード手段と、
- 前記ホームコントロールネットワークデバイス(61)の前記一意の端末のペア(42、42b、41c)へのエンドツーエンドのデータ転送接続を確立するための前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末のペア(42、42b)のネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)に要求するためのコード手段と、
- 前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末のペア(42、42b)の前記ネットワーク経路情報を前記ホームコントロールネットワークサーバ(21)から受信するためのコード手段と、
- 受信されたネットワーク経路情報を用いて、前記ホームコントロールネットワークデバイス(61)の前記一意のネットワーク端末のペア(42、42b)とともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワーク(55)を確立するためのコード手段とを含み、前記仮想プライベートネットワーク(55)には前記ホームコントロールネットワークサーバ(21)が属さないことを特徴とする、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、建物内のアクチュエータの遠隔制御方法と、そのコンポーネントを備える遠隔制御システムとに関する。

【背景技術】
【０００２】
遠隔制御可能なデバイスおよびシステムが、建物および家に設置されることが増えている。システムの目的は、それらの建物内に住むことが安全かつ快適であるように建物内の状態を保証および/または維持することである。遠隔で監視されるデバイスの遠隔制御の範囲は幅広い。同じ建物が、複数の供給者からのデバイスを有する可能性がある。これらのデバイスは、互いに直接通信することができないことが多い。各システムは、独自の動作ロジックを有しており、システムの遠隔制御が、特定のデータ通信ソリューションを使用することを必要とすることもよくある。
【０００３】
近年、建築設備(building service)の供給者は、特定の対象(target)に固有の合意された機能を含み、電話ネットワークか、または永続的もしくは無線2G/3Gネットワークブロードバンド接続である可能性があるブロードバンドネットワークかのどちらかを介して別に維持されなければならない別にコストのかかる追加の接続を、顧客の対象のために事業者(operator)が自身で注文することによりこの問題を非常に広く解決することを始めている。ほとんどの供給者は、いくつかの問題点を含むものの、これが今のところそれらの供給者にとって最も簡単な運用の形態であることが分かっている。
【０００４】
新しい追加の接続が対象のために提供される場合、データ通信の問題が、ローカルのイントラネットの管理者と別途合意されなければならないことが多い。イントラネットの管理者は、おそらく、遠隔接続が正常に確立され得るように、接続のための追加のネットワーク設定を行わなければならない。
【０００５】
建築設備の供給者は、追加の接続、特に永続的なネットワーク接続を長時間、ときには何週間も待たなければならないことが多い。接続が最終的に受け取られるとき、事業者から接続を注文されたときに合意されたように接続が機能せず、建築設備の供給者が修正手順について交渉し、事業者が問題に対応するのを待たなければならない。
【０００６】
さらに、事業者は、無線ブロードバンド接続の動作について話すときに多くのことを約束し過ぎる。遠隔の対象が新しい無線接続に接続され、それが正しく機能しないとき、大抵の場合、長期の、時間がかかり、コストがかかり、すべてにおいて大変な交渉が待ち受けている。
【０００７】
加えて、事業者は、モデムと、例えば、24ヶ月の義務的な使用時間とを接続と抱き合わせにして顧客を接続ユーザにしようと努める。しかし、すべてのユーザがこれに参加したいわけではなく、「自分達自身が決定権を持ちたい」と思っていることが多い。
【０００８】
建築設備の供給者は、さらに、アプリケーションに固有のソリューションによって対象の遠隔使用を解決しようとする可能性がある。したがって、デバイスの供給者は、事業者から独自の無線ネットワークを買い、その無線ネットワーク内でプライベートアクセスポイント名(APN)を形成する可能性があり、それにより、GPRS(汎用パケット無線サービス: General Packet Radio Service)およびHSDPA(高速ダウンリンクパケットアクセス: HighSpeed Downlink Packet Access)/HSUPA(高速アップリンクパケットアクセス: HighSpeed Uplink Packet Access)ネットワークのデータ通信の設定を決定する。APN設定を使用することによって、インターネット接続が、対象のデバイスに無線2G/3G/4Gネットワークを介して提供される。そのような場合、ユーザは、接続と、その遠隔使用を可能にするインターフェースモデムおよびプログラムとの料金を別途支払わなければならない。多くの場合、そのような追加の接続は、2つ以上の使用目的、例えば、建築設備の供給者によって供給されるデバイスの遠隔使用のために使用できないか、または使用されない可能性がある。さらに、最近は、概して、事業者が、そのような接続の最大データ転送量を制限してお

り、その最大データ転送量を超えるとき、接続の所有者に多額の追加の請求書が発生する可能性がある。

【０００９】

いくつかの建物を所有する住宅協同組合型の対象においては、建物が、建物間で形成されたイントラネット内でのみ行われる「遠隔使用」に接続される可能性がある。遠隔で接続するユーザが物理的にイントラネット内の問題の建物のうちの1つの中以外の場所にいる場合、そのような対象に関する本当の遠隔の接続は得られない。

【発明の概要】

【発明が解決しようとする課題】

【００１０】

建物および家に既に存在するインターネット接続が建築設備および監視の遠隔使用でそのまま利用される、建物内の技術的なデバイスのための新しい遠隔制御の構成と、この遠隔制御の構成を利用する遠隔制御方法とを提供することが、本発明の目的である。本発明による遠隔使用デバイスのペアによって、建物の対象の接続が、それ自体で遠隔使用に適するように変更される。対象および対象の中のイントラネットのデータネットワーク接続の既存の機能は変更されない。

【課題を解決するための手段】

【００１１】

本発明の目的は、建物内に固定的に設置されたホームコントロールネットワークデバイス(home control network device)と、建物の監視を実施する人のホームコントロールネットワークキー(home control network key)とが、それらが本発明によるホームコントロールネットワークサーバ(home control network server)から受信した連絡先情報に基づいてインターネットを介した安全な双方向接続を確立するデバイス構成によって達成される。建物内の遠隔制御または遠隔監視されるべきデバイスが接続される建物内のホームコントロールネットワークデバイスは、建物内のデータネットワーク接続デバイス/ネットワーク端末、例えばモデムに接続される。

【００１２】

ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーの現在のIPアドレスは、本発明に関連するホームコントロールネットワークサーバに保持されており、それらのIPアドレスが、前記デバイス間の接続を確立するために使用される。本発明による追加の手順および接続確立方法によって、前記デバイスの両方は、何らかのプライベートな、非パブリックネットワークに接続される可能性があり、さらに、それら自体の間でインターネットを介したデータ転送接続を確立することができる。有利なことに、ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーが同時に非パブリックIPアドレスしか持たないとしても、確立された接続である時点で前記デバイスがパブリックIPアドレスをさらに取得すれば、移動できるホームコントロールネットワークキーと固定的に設置されたホームコントロールネットワークデバイスとの間のインターネットを介したデータ転送接続を確立するのに十分である。ホームコントロールネットワークサーバは、デバイスが利用できるようにデバイスのIPアドレスを送信した後、実際のデータ転送接続の確立には関与しない。

【００１３】

本発明による建物の遠隔制御システムの利点は、ホームコントロールネットワークデバイスのペアの両方のデバイスが、それらのデバイスが置かれた位置から、インターネットに接続する建物のデバイスのIPアドレスへのそれらのデバイスのルーティングを探すことができ、探したルートを、それらのデバイスのペアの識別情報およびIPアドレスに関してインターネット上の別のホームコントロールネットワークサーバに記憶することができることである。

【００１４】

本発明によるそれぞれのホームコントロールネットワークデバイスのペアが、それら自体の間で独立に、ネットワーク内で互いを特定する所定の一意のデバイスのペアまたはデ

バイスのグループを形成することが、本発明のさらなる利点である。この特定方法によって、ユーザとともに持ち運ばれるホームコントロールネットワークキー、またはホームコントロールネットワークキーの機能を実装する、何らかのデータ処理デバイスにインストールされたコンピュータプログラムは、それ自体の一意のホームコントロールネットワークデバイスのペアを用いてのみネットワーク接続を確立し、いかなるその他のネットワークデバイスとの接続も確立できない。したがって、ホームコントロールネットワークキーは、建物の「ネットワークの扉」の安全性の高いキーとして機能する。

【００１５】

本発明による遠隔制御システムのデバイスのペアが、ホームコントロールネットワークサーバのアドレス情報の助けを借りてそれら自体の間で独立に、確立された接続が外部サーバを通じてまったく循環することなく、サービスを提供するローカルネットワークデバイスおよびインターネット(VPN: 仮想プライベートネットワーク)を通じて、直接的な双方向の安全なOSIモデル(開放型システム間相互接続参照モデル)のデータリンク層(レイヤ2)またはさらにネットワーク層(レイヤ3)レベルのデータ転送接続を確立することができることが、本発明のさらなる利点である。データリンク層レベルの安全な遠隔転送接続は、建築設備制御デバイスの多くの柔軟な使用および利用のための基本要件である。

【００１６】

ホームコントロールネットワークデバイスのペアが、製造に関連してか、または後で行われるスタートアップに関連してかのどちらかで確立され得ることが、本発明のさらなる利点である。どちらの場合も、有利なことに、デバイスのペアは、例えば、USBポートを介してホームコントロールネットワークデバイスとホームコントロールネットワークキーとを1つに接続することによって形成され、それによって、ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーのどちらかまたは両方が、互いの識別コードを受信する。

【００１７】

本発明による遠隔制御システムにおいては、ホームコントロールネットワークキーのプログラムが、それらのセキュリティ識別子およびパスワードとともに外部サーバに記憶される可能性があり、その外部サーバから、それらのプログラムが、新しい遠隔制御ネットワークキー(remote control network key)、または端末にインストールされたプログラムに取り出される可能性があり、そのプログラムが、セキュリティ識別子またはパスワードに応えてホームコントロールネットワークキーをシミュレートすることが、本発明のさらなる利点である。

【００１８】

本発明によるホームコントロールネットワークキーは、プロセッサ、メモリ、およびメモリに記憶されたコンピュータプログラムコードを含む可能性があり、それらのプロセッサ、メモリ、およびメモリに記憶されたコンピュータプログラムコードが、

- ホームコントロールネットワークキーおよびネットワーク端末のペアが入力/出力手段によって1つに接続されるときに、ホームコントロールネットワークキーのネットワーク端末のペアによって送信されたデバイス識別コードを受信し、ホームコントロールネットワークキー自体のデバイス識別コードをホームコントロールネットワークキーのネットワーク端末のペアに送信し、
- ホームコントロールネットワークキーからインターネットへのネットワーク経路を判定し、
- 判定されたネットワーク経路を、ホームコントロールネットワークキーのメモリと、ホームコントロールネットワークサーバのメモリとの両方に記憶し、
- ホームコントロールネットワークキーのネットワーク端末のペアへのエンドツーエンドのデータ転送接続を確立するためのホームコントロールネットワークキーのネットワーク端末のペアのネットワーク経路情報をホームコントロールネットワークサーバに要求し、
- ホームコントロールネットワークキーのネットワーク端末デバイスのペアのネットワーク経路情報をホームコントロールネットワークサーバから受信し、

- 受信されたネットワーク経路情報の助けを借りて、ホームコントロールネットワークキーのネットワーク端末のペアとともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワークを確立するように構成され、仮想プライベートネットワークにはホームコントロールネットワークサーバが属さないことを特徴とする。

【００１９】

本発明による建物のホームコントロールネットワークデバイスは、そのプロセッサ、メモリ、およびメモリに記憶されたコンピュータプログラムコードが、

- ホームコントロールネットワークデバイスおよびネットワーク端末のペアが入力/出力手段によって1つに接続されるときに、ホームコントロールネットワークデバイスのネットワーク端末のペアによって送信されたデバイス識別コードを受信するか、またはホームコントロールネットワークデバイス自体のデバイス識別コードをホームコントロールネットワークデバイスのネットワーク端末のペアに送信し、
- ホームコントロールネットワークデバイスからインターネットへのネットワーク経路を判定し、
- 判定されたネットワーク経路を、ホームコントロールネットワークデバイスのメモリと、ホームコントロールネットワークサーバのメモリとの両方に記憶し、
- ホームコントロールネットワークデバイスの端末のペアへのエンドツーエンドのデータ転送接続を確立するためのホームコントロールネットワークデバイスのネットワーク端末のペアのネットワーク経路情報をホームコントロールネットワークサーバに要求し、
- ホームコントロールネットワークデバイスのネットワーク端末デバイスのペアのネットワーク経路情報をホームコントロールネットワークサーバから受信し、
- 受信されたネットワーク経路情報の助けを借りて、ホームコントロールネットワークデバイスのネットワーク端末のペアとともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワークを確立するように構成され、仮想プライベートネットワークにはホームコントロールネットワークサーバが属さないことを特徴とする。

【００２０】

ホームコントロールネットワークキーで利用される、本発明によるコンピュータプログラムは、

- ホームコントロールネットワークキーおよびネットワーク端末のペアが入力/出力手段によって1つに接続されるときに、ネットワーク端末のペアによって送信されたデバイス識別コードを受信するか、またはホームコントロールネットワークキー自体のデバイス識別コードをネットワーク端末のペアに送信するためのコード手段と、
- ホームコントロールネットワークキーからインターネットへのネットワーク経路を判定するためのコード手段と、
- 判定されたネットワーク経路を、ホームコントロールネットワークキーのメモリと、ホームコントロールネットワークサーバのメモリとの両方に記憶するためのコード手段と、
- ネットワーク端末のペアへのエンドツーエンドのデータ転送接続を確立するためのネットワーク端末のペアのネットワーク経路情報をホームコントロールネットワークサーバに要求するためのコード手段と、
- ネットワーク端末のペアのネットワーク経路情報をホームコントロールネットワークサーバから受信するためのコード手段と、
- 受信されたネットワーク経路情報を用いて、ネットワーク端末のペアとともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワークを確立するためのコード手段とを含み、仮想プライベートネットワークにはホームコントロールネットワークサーバが属さないことを特徴とする。

【００２１】

ホームコントロールネットワークデバイスで利用される、本発明によるコンピュータプログラムは、

- ホームコントロールネットワークデバイスおよびネットワーク端末のペアが入力/出力手段によって1つに接続されるときに、ホームコントロールネットワークデバイスのネッ

トワーク端末のペアによって送信されたデバイス識別コードを受信するか、またはホームコントロールネットワークデバイス自体のデバイス識別コードをホームコントロールネットワークデバイスのネットワーク端末のペアに送信するためのコード手段と、
- ホームコントロールネットワークデバイスからインターネットへのネットワーク経路を判定するためのコード手段と、
- 判定されたネットワーク経路を、ホームコントロールネットワークデバイスのメモリと、ホームコントロールネットワークサーバのメモリとの両方に記憶するためのコード手段と、
- ホームコントロールネットワークデバイスのネットワーク端末のペアへのエンドツーエンドのデータ転送接続を確立するためのホームコントロールネットワークデバイスのネットワーク端末のペアのネットワーク経路情報をホームコントロールネットワークサーバに要求するためのコード手段と、
- ホームコントロールネットワークデバイスのネットワーク端末のペアのネットワーク経路情報をホームコントロールネットワークサーバから受信するためのコード手段と、
- 受信されたネットワーク経路情報を用いて、ホームコントロールネットワークデバイスのネットワーク端末のペアとともに、建物のアクチュエータの遠隔制御のための仮想プライベートネットワークを確立するためのコード手段とを含み、仮想プライベートネットワークにはホームコントロールネットワークサーバが属さないことを特徴とする。

【００２２】

本発明のいくつかの有利な実施形態は、従属請求項に示される。

【００２３】

本発明の基本的な概念は、以下の通りである。何らかの建物において遠隔制御を実施するために、デバイスのペア、ホームコントロールネットワークデバイスおよびホームコントロールネットワークキー(デバイス)が製造され、少なくとも1つのホームコントロールネットワークデバイスおよび少なくとも1つのホームコントロールネットワークキー(デバイス)は、お互いとだけデータ転送接続を確立することができる。前記ホームコントロールネットワークキー(デバイス)は、この目的のために製造された別個の電子デバイスであるか、またはさらにはホームコントロールネットワークキーの機能を実装する本発明によるコンピュータプログラムがインストールされた何らかのデータ処理デバイスであるかのどちらかである可能性がある。

【００２４】

遠隔制御されるべき建物内のホームコントロールネットワークデバイスは、制御されるべき建物内の既存のイントラネットネットワークまたはインターネットネットワークに設置される。ホームコントロールネットワークデバイスは、イントラネットまたはインターネットネットワークにおいて1つのサブネットワーク、制御イントラネットネットワークを確立し、この制御イントラネットネットワークに、建物内の制御されるべきさまざまなアクチュエータが、有線データ転送接続かまたは無線データ転送接続かのどちらかによって接続される。

【００２５】

本発明の1つの有利な実施形態においては、個々のホームコントロールネットワークキーまたはいくつかのホームコントロールネットワークキーが、異なる建物内の2つ以上のホームコントロールネットワークデバイスのデバイスのペアとして機能する可能性がある。ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーの識別コードが、それらの製造に関連して前記デバイスに記憶されるか、または前記デバイスが、例えばそれらのUSBポートのうちの1つに接続されるときにそれらの識別コードを変更する。識別コードを使用することによって、ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーは、それらの間で安全な双方向データ転送接続を確立することができる。有利なことに、データ転送接続は、OSIモデルのデータリンク層(レイヤ2)またはネットワーク層(レイヤ3)に基づく可能性がある。

【００２６】

スタートアップに関連して、両方のデバイスは、それらが位置するネットワークからインターネットに接続されたネットワーク端末に至るまでのデバイスのルーティング情報を判定し、そのルーティング情報は、接続を確立するために必要とされる。このルーティング情報は、インターネットに接続された本発明によるホームコントロールネットワークサーバに記憶される。ホームコントロールネットワークキーは、何らかの建物内のそのデバイスのペアへのインターネットを介したデータ転送接続を確立したいとき、ホームコントロールネットワークサーバから、そのペアとして機能するホームコントロールネットワークデバイスのルーティング情報を取得する。取得されたルーティング情報を利用することによって、ホームコントロールネットワークキーは、直接的なエンドツーエンドのデータ転送接続の確立を開始する。直接的なデータ転送接続が確立されたとき、有利なことにネットワーク層を使用する直接的なVPNデータ転送接続が、ホームコントロールネットワークキーと建物内のホームコントロールネットワークデバイスとの間で確立されている。

【００２７】

本発明によるホームコントロールネットワークデバイスは、建物の制御および管理に関連する既存の内部データ転送ネットワークと、建物からインターネットにトラフィックを中継するネットワーク端末との間の、遠隔制御されるべき建物の内部データ転送ネットワークに設置される。建物の制御に関連するすべてのデバイスは、ホームコントロールネットワークデバイスの入力に接続され、ホームコントロールネットワークデバイスの出力は、インターネットのトラフィックを中継するネットワーク端末のイントラネットデバイスの入力手段に接続される。

【００２８】

本発明によるホームコントロールネットワークキーは、インターネットへのデータ転送接続を確立することができる何らかのデータ転送デバイスに接続され得る。あり得るデータ転送デバイスは、例えば、PC、タブレットコンピュータ、またはスマートフォンである。データ転送デバイスへのホームコントロールネットワークキーの接続は、例えば、LANインターフェース(ローカルエリアネットワーク)、WLANインターフェース(無線LAN)、WANインターフェース(広域ネットワーク)、USBインターフェース(ユニバーサルシリアルバス)、またはアンテナインターフェースの助けを借りて行われ得る。

【００２９】

本発明の1つの有利な実施形態においては、ホームコントロールネットワークキーの機能を実装するコンピュータプログラムが、ポータブルデータストレージ手段、例えば、USBスティックに記憶され、そのポータブルデータストレージ手段から好適なデータ処理デバイスにコンピュータプログラムがインストールされ得る。データ処理デバイスにインストールされたプログラムは、ホームコントロールネットワークキーのすべての機能をシミュレートする。

【００３０】

ホームコントロールネットワークキーが、ローカルネットワークに接続されたデータ転送デバイスに接続されるか、またはホームコントロールネットワークキーの機能を実装するコンピュータプログラムが、前記データ転送デバイスにインストールされるかのどちらかのとき、ホームコントロールネットワークキーは、最初に、ホームコントロールネットワークサーバへの異なるサブネットワークを通じたホームコントロールネットワークキー自体のルーティングを判定する。ルーティングが突き止められるとき、ホームコントロールネットワークキーのルーティング情報が、本発明によるホームコントロールネットワークサーバに記憶される。

【００３１】

双方向のエンドツーエンドデータ転送チャネルがホームコントロールネットワークキーとホームコントロールネットワークデバイスとの間で形成されるとき、ホームコントロールネットワークサーバに記憶された異なるサブネットワークを通るデバイスのペアのルーティング情報が、データ転送チャネルを形成するために利用される。データ転送接続が確立されたとき、データ転送は、ホームコントロールネットワークサーバがデータ転送にも

はやまったくかかわらないように行われる。

【００３２】

以下で、本発明が詳細に説明される。説明において、添付の図面に対する参照がなされる。

【図面の簡単な説明】

【００３３】

【図１】本発明による双方向データ転送接続が、遠隔制御を扱うクライアントデバイスと、建物の個々の制御および管理デバイスとの間でどのようにして確立され得るかを一例として示す図である。

【図２】双方向データ転送接続が、遠隔制御を扱うクライアントデバイスと、建物の個々の制御および管理デバイスとの間で確立され得る、本発明による第2の例を示す図である。

【図３】クライアントデバイスと建物内のデバイスとの間のデータ転送接続がどのようにして確立されるかを例示的な流れ図として示す図である。

【図４】本発明によるホームコントロールネットワークデバイスを一例として示す図である。

【図５ａ】本発明によるホームコントロールネットワークキーを一例として示す図である。

【図５ｂ】本発明によるホームコントロールネットワーク2重キー(home control network double key)を一例として示す図である。

【図６】本発明によるホームコントロールネットワークサーバを一例として示す図である。

【発明を実施するための形態】

【００３４】

以下の説明の実施形態は、例としてのみ与えられ、当業者は、説明に記載された方法とは異なる何らかの別の方法で本発明の基本的な概念を実施することもできる。説明はいくつかの個所で特定の1つの実施形態または複数の実施形態に言及する可能性があるが、これは、その言及が1つの説明された実施形態のみを対象とすること、または説明された特徴が1つの説明された実施形態でのみ使用できることを意味しない。2つ以上の実施形態の個々の特徴が組み合わされる可能性があり、したがって、本発明の新しい実施形態が提供され得る。

【００３５】

図1および2は、本発明による遠隔制御システムの2つの有利な実施形態1Aおよび1Bを示す。図1および2の例においては、1つのホームコントロールネットワークキー42、またはソフトウェアによってホームコントロールネットワークキーに変換されたデータ処理デバイス41cが、何らかの建物内の1つのホームコントロールネットワークデバイス61へのデータ転送接続を確立するために使用される。しかし、有利なことに、本発明によるホームコントロールネットワークキー42、またはホームコントロールネットワークキーに変換されたデータ処理デバイス41cは、2つ以上の建物内の別個のホームコントロールネットワークデバイスとともに機能することもできる。

【００３６】

図1および2の両方の実施形態において、データ転送ネットワークは、主として、同じ基本的なネットワーク構造を有する。図1および2の両方において、参照番号2によってインターネットが示されている。何らかのパブリックネットワークまたはイントラネット、参照番号3も、インターネット2に接続される。ネットワーク3は、永続的または無線データ転送ネットワークである可能性がある。図1において、第1のデータ転送ネットワーク4、建物のハウスコントロール遠隔ネットワーク(house control remote network)が、ネットワーク3に接続されており、そのハウスコントロール遠隔ネットワークに、遠隔制御を実施するクライアントデバイス、参照番号41aが接続され得る。図2においては、ホームコントロールネットワークキーをシミュレートするデータ処理デバイス41cが、パブリックネ

ットワーク/イントラネットネットワーク3に接続される。

【００３７】

遠隔制御されるべき建物のハウスイントラネット(house intranet)が、図1および2において、参照番号5で示されている。第2のデータ転送ネットワーク6、本発明によるハウスコントロールイントラネット(house control intranet)が、ハウスイントラネットネットワーク5に接続される。建物内の遠隔制御されるべきアクチュエータ62～65が、ハウスコントロールイントラネットに接続される。

【００３８】

本発明によるホームコントロールネットワークデバイス61および/またはホームコントロールネットワークキー42もしくは41cとインターネット2との間に、図1および2に示されているサブネットワークとは異なるより多くのサブネットワークも存在し得ることは、当業者に明らかである。

【００３９】

図1および2の例においては、本発明による第2のネットワーク端末、ホームコントロールネットワークデバイス61(HCND)が、ハウスイントラネットネットワーク10.0.0.0/24、参照番号5に接続される。ハウスイントラネットネットワーク5は、ネットワーク端末51によってインターネット2に接続される。ネットワーク端末51は、ネットワークアドレストランスレータNATも含み得るルータ、モデム、またはファイアウォールである可能性がある。図1および2の例において、ハウスイントラネット5は、NAT機能を含むファイアウォールFW1、参照番号51の裏にある。ファイアウォールFW1のパブリックIPアドレスは、図1および2の例においては240.1.1.2である。ハウスイントラネット5内で、ファイアウォールFW1の内部IPアドレスは10.0.0.1である。2つの例示的なその他のデータ処理デバイスも、ハウスイントラネットネットワーク5に接続されており、ハウスイントラネットネットワーク内でのそれらのデータ処理デバイスのIPアドレスは、10.0.0.3および10.0.0.4である。

【００４０】

ハウスコントロールイントラネットネットワーク172.17.0.0/24(HCI)、参照番号6は、ホームコントロールネットワークデバイス61を介してハウスイントラネットネットワーク5に接続される。ハウスコントロールイントラネットネットワークでのホームコントロールネットワークデバイス61のIPアドレスは172.17.0.1であり、ハウスイントラネットネットワークでのホームコントロールネットワークデバイス61のIPアドレスは10.0.0.2である。図1および2の例においては、4つの例示的なデバイス/サーバ62、63、64、および65が、ハウスコントロールイントラネット6に接続される。それらのデバイス/サーバは、永続的な接続かまたは無線データ転送接続かのどちらかでハウスコントロールイントラネット6に接続され得る。

【００４１】

参照番号62は、照明制御ウェブサーバを示し、ハウスコントロールイントラネットネットワークでのその照明制御ウェブサーバのIPアドレスは172.17.0.5である。遠隔ユーザに対して、照明制御ウェブサーバ62は、デバイスHCND4として見られる。

【００４２】

参照番号63は、暖房制御ウェブサーバを示し、ハウスコントロールイントラネットネットワークでのその暖房制御ウェブサーバのIPアドレスは172.17.0.4である。遠隔ユーザに対して、暖房制御ウェブサーバ63は、デバイスHCND1として見られる。

【００４３】

参照番号64は、監視カメラウェブサーバを示し、ハウスコントロールイントラネットネットワークでのその監視カメラウェブサーバのIPアドレスは172.17.0.3である。遠隔ユーザに対して、監視カメラウェブサーバ64は、デバイスHCND2として見られる。

【００４４】

参照番号65は、空調ウェブサーバを示し、ハウスコントロールイントラネットネットワークでのその空調ウェブサーバのIPアドレスは172.17.0.2である。遠隔ユーザに対して、

空調ウェブサーバ65は、デバイスHCND3として見られる。

【００４５】

図1の例において、本発明による第1のネットワーク端末、ホームコントロールネットワークキー42(HCNK)は、ハウスコントロール遠隔ネットワーク172.17.0.0/24、参照番号4に接続される。ハウスコントロール遠隔ネットワーク4は、イントラネット3のファイアウォールFW1、参照番号31の裏にある。NATファイアウォール31のパブリックIPアドレスは、この例においては240.2.1.2であり、NATファイアウォールの内部IPアドレスは、10.0.1.1である。

【００４６】

ハウスコントロール遠隔ネットワーク172.17.0.0/24(HCRN)、参照番号4は、本発明によるホームコントロールネットワークキー42を介してデータ転送ネットワーク3に接続される。イントラネットネットワークでのホームコントロールネットワークキー42のIPアドレスは10.0.1.2であり、ハウスコントロール遠隔ネットワークでのホームコントロールネットワークキー42のIPアドレスは172.17.0.6である。図1および2の例においては、例示的なデータ処理デバイス41aがハウスコントロール遠隔ネットワーク4に接続され、ハウスコントロール遠隔ネットワーク4でのそのデータ処理デバイスのIPアドレスは172.17.0.7である。このデータ処理デバイス41aは、ハウスコントロールイントラネットネットワーク6に接続されたデバイス/サーバ62、63、64、または65を遠隔制御することが望ましいときに使用される。

【００４７】

本発明によるホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61は、それらが、データリンク層またはネットワーク層に基づくエンドツーエンドのデータ転送接続、図1および2の例においてはVPNデータ転送接続55をそれらの間で確立することができるように、互いのルーティング情報を必要とする。ルーティング情報は、本発明のホームコントロールネットワークキー42とホームコントロールネットワークデバイス61との両方によってインターネット上のホームコントロールネットワークサーバ21(HCNS)に記憶される。

【００４８】

図1の例において、NATファイアウォールは、発信されるUDP通信を完全には制限しない。それらのNATファイアウォールは、必要がなければUDP接続(ユーザデータグラムプロトコル)の送信元ポート番号を予測できない形で変更することもない、1つの状態の、「記憶付きの(with memory)」いわゆるNATファイアウォールである。図1の例において、目的は、ホームコントロールネットワークキー42とホームコントロールネットワークデバイス61との間に、データリンク層で、イーサネット(登録商標)レベルの接続を確立することである。

【００４９】

図1による遠隔制御システム1Aにおいて、デバイス間の、仮想プライベートネットワーク(VPN)に属するデータ転送接続55を確立することが望ましいとき、デバイス42と61との両方が、ホームコントロールネットワークサーバ21から、相手のデバイスによってホームコントロールネットワークサーバ21に記憶されたルーティング情報を取得する。ルーティング情報を渡す前に、ホームコントロールネットワークサーバ21は、それが本当に許可されたホームコントロールネットワークキー/ホームコントロールネットワークデバイスのペアの問いであることを調べる。取得されたルーティング情報の助けを借りて、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61は、それらの間で直接的なVPN接続を確立する。VPN接続55が完成しているとき、ハウスコントロール遠隔ネットワーク4のデータ処理デバイス41aが、ハウスコントロールネットワーク6のデバイス62、63、64、または65に連絡することができる。

【００５０】

データ転送接続を確立することが可能であるためには、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61が、それら自体のネットワー

クから少なくともインターネット2までのそれらのネットワーク経路を決定しなければならない。このネットワーク経路の決定は、例えば、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61が有利に利用する以下の方法でなされ得る。

【００５１】

DHCPプロトコル(動的ホスト構成プロトコル)によって、データ処理デバイスのネットワークインターフェースのIP設定が取得され得る。DHCPプロシージャによって取得可能な設定は、少なくとも、データ処理デバイスのIPアドレス、ネットワークマスク、デフォルトゲートウェイ、およびドメイン名をIPアドレスに変換するDNSサーバ(ドメインネームシステム)である。

【００５２】

Tracerouteプロシージャは、TCP/IPプロトコルを使用するツールであり、どのルートまたはネットワーク経路に沿ってパケットが決められたマシンに転送されるかを判定する。Tracerouteプロシージャでは、ネットワークに接続されたデータ転送デバイスが、そのデータ転送デバイスが送信するパケットの「生存時間」の値(TTL)を、0から開始して、一度に1ずつ足していくことによってネットワーク経路を突き止める。

【００５３】

概して、ネットワーク経路を突き止めることは、以下のようにして行われる。データ処理デバイスが、TTL値「0」を用いて、外部ネットワーク内の何らかの送信先アドレスを有するIPパケットをデフォルトゲートウェイに送信する。デフォルトゲートウェイは、TTL失効(TTL expired)のメッセージでこれに応答する。例えば、このメッセージから、デフォルトゲートウェイのIPアドレス、遅延などが明らかになる。

【００５４】

その後、データ処理デバイスが、TTL値「1」を用いて、外部ネットワーク内の何らかの送信先アドレスを有するIPパケットをデフォルトゲートウェイに送信する。やはり、デフォルトゲートウェイの次のルータが、「TTL失効」メッセージで応答し、この応答から、この次の(2番目の)ルータのIPアドレスが分かる。この送信/応答プロセスが、所望の目的の場所に到達するまで、TTL値を増やすことによって続けられる。インターネットの場合、通常、TTL値6～15で最終的な目的の場所に到達する。結局、データ処理デバイスが、外部、例えばインターネットへのネットワーク経路を知る。

【００５５】

ICMPプロトコル(インターメット制御メッセージプロトコル)が、外部アドレスを突き止める際に使用され得る。ICMPパケットのルート記録(Record Route)フラグがICMPプロシージャで使用され、そのフラグが、ネットワーク経路上のデバイスのオペレーティングシステムに、送信しているルータのIPアドレスを、ICMPパケットのタイトル(title)に記録するように要求する。

【００５６】

図1の例においては、ネットワーク経路判定は、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61によって、上述のプロセスのうちの少なくとも1つを用いて行われる。これらのデバイスは、発見されたネットワーク経路をホームコントロールネットワークサーバ21に記憶し、そのホームコントロールネットワークサーバ21がそのメモリにそれらを記憶する。

【００５７】

有利なことに、本発明によるホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61は、空きサイバースペースを判定する機能も有する。前記デバイスは、ホームコントロールネットワークサーバ21上のネットワーク経路情報を利用することによって、利用可能なサイバースペースを、自動的に、それら自体のために判定するように構成されている。前記デバイスは、ホームコントロールネットワークサーバ21に、サイバースペースの何らかの空いている部分を与えるように要求する。ホームコントロールネットワークサーバ21は、受信したネットワーク経路を調べ、それによって知ら

れたいかなるデバイスのネットワーク経路にも1つのアドレスも載っていない何らかのネットワークのブロックを返す。

【００５８】

有利なことに、さらに、ホームコントロールネットワークデバイス61は、それ自体のサブネットワーク4および6内で、そのサブネットワーク4に接続されたデバイスのためにDHCPおよびDNSサービスを提供する。加えて、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61は、サブネットワークに接続されたデバイスのためのデフォルトゲートウェイとして機能する。

【００５９】

図2は、本発明による別の遠隔制御システム1Bを示す。図2においては、ユーザによって利用されるデータ処理デバイス41cが、参照番号3によって示されるデータ転送ネットワークに接続される。図2の実施形態は、図1のホームコントロールネットワークキー42の機能が、クライアントによって利用されるデータ処理デバイス41cに接続され得るUSBメモリ42bで置き換えられる点で図1の実施形態と異なる。この実施形態においては、データ処理デバイス41cおよびUSBメモリ42bが、一緒に、ホームコントロールネットワークキーを形成する。

【００６０】

本発明の別の有利な実施形態においては、本発明によるホームコントロールネットワークキーの機能を実装するコンピュータプログラムが、USBメモリ42bからデータ処理デバイス41cにインストールされる。有利なことに、コンピュータプログラムは、例えば、USBスティック42bをデータ処理デバイス41cのUSBポートに接続することによって、USBスティック42bからデータ処理デバイス41cに記憶され得る。当業者には、何らかのその他の従来技術のデータストレージ手段もコンピュータプログラムのためのストレージ手段として使用され得ることは明らかである。この実施形態においては、データ処理デバイス41cが、データ処理デバイス41cにインストールされたコンピュータプログラムによって本発明によるホームコントロールネットワークキーをシミュレートする。

【００６１】

図2においては、図1のホームコントロールネットワークキー42が、すべてまたは部分的にユーザのデータ処理デバイス41cでシミュレートされる。ユーザが、そのユーザのデータ処理デバイス41cのブラウザによってこのシミュレーションソフトウェアに接続するか、または代替的に、シミュレーションソフトウェアが、データ処理デバイス41cのブラウザウィンドウを開く。シミュレーションは、データ処理デバイス41cにおいて本発明によるシミュレーションプログラムを起動することによって開始され、シミュレーションプログラムは、物理的なホームコントロールネットワークキー42のすべての機能をソフトウェアによって実装する。

【００６２】

この実施形態においては、図1のホームコントロールネットワークキー42のすべての機能、通信、スタートアップ、および接続の確立が、ユーザのデータ処理デバイス41cによって実施され、それによって、図1による物理的に分かれたホームコントロールネットワークキー42は、建物内のデバイスのペア61への接続を確立するために必要とされない。

【００６３】

何らかの理由で、そのような直接的なVPNトンネルの確立が、図1および2に示されたホームコントロールネットワークキー42、42b、もしくは41cとホームコントロールネットワークデバイス61との間で成功しないか、またはときどきしか成功しない場合、説明された遠隔制御の構成は、インターネット2に接続されたホームコントロールネットワーク2重キーを利用することができ、ホームコントロールネットワーク2重キーは、接続の確立および維持を支援する。そのような遠隔制御システムにおいては、ホームコントロールネットワーク2重キーが、異なる方向から来る2つのVPNトンネルを1つのVPNトンネルへとブリッジすることによってVPNトンネルの生成を支援する。クライアントデバイスのユーザにとっては、遠隔制御システムは、図1または図2に示された遠隔制御システムと同じように機

能する。

【００６４】

以下は、図1の例の本発明による遠隔制御システム1Aの動作の例である。

【００６５】

ホームコントロールネットワークデバイス61:

【００６６】

ホームコントロールネットワークデバイス61は、例えば、ホームコントロールネットワークデバイス61のWANポートにケーブルをつなぐことによって10.0.0.0/24のネットワーク(ハウスイントラネット5)に接続される。ホームコントロールネットワークデバイス61は、DHCPプロシージャによってそのIP設定を自動的に取得する。有利なことに、ハウスイントラネットネットワーク5のファイアウォールFW1がDHCPサーバとして機能し、そのファイアウォールが、24ビットのネットワークマスク(255.255.255.0)でIPアドレス10.0.0.2をホームコントロールネットワークデバイス61に与える。DHCPサーバは、デフォルトルータアドレス10.0.0.1およびDNSサーバアドレス10.0.0.1も与える。

【００６７】

ホームコントロールネットワークデバイス61は、DNSサーバの助けを借りて、ホームコントロールネットワークサーバ21(HCNS、DNSアドレスetahallinta.fi)のIPアドレスを突き止めることによって通信を開始する。DNSサーバ10.0.0.1は、ホームコントロールネットワークサーバ21のIPアドレスを240.1.1.1として与える。

【００６８】

ホームコントロールネットワークデバイス61は、TCPまたはUDPプロトコルを用いてインターネットを介してホームコントロールネットワークサーバ21に連絡する。ホームコントロールネットワークデバイス61は、製造に関連して決められた証明書および/またはパスワードによって、ホームコントロールネットワークサーバ21との相互の動作権限を認証する。有利なことに、このデータ転送接続は、例えば、SSL/TLS暗号化によって暗号化される。ホームコントロールネットワークサーバ21は、着信する接続から、図1の例においては240.1.1.2である、ホームコントロールネットワークデバイス61のパブリックIPアドレスを知る。ホームコントロールネットワークデバイス61は、ホームコントロールネットワークサーバ21に、そのホームコントロールネットワークデバイス61自体のアドレスおよびネットワークマスク(10.0.0.2/24)を知らせる。ホームコントロールネットワークサーバ21は、そのデータベースにこの情報を記憶する。

【００６９】

有利なことに、ホームコントロールネットワークデバイス61は、ホームコントロールネットワークサーバ21へのtraceroute操作も実行し、発見されたネットワーク経路をホームコントロールネットワークサーバ21にレポートする。ホームコントロールネットワークサーバ21は、そのデータベースに、ホームコントロールネットワークデバイス61の受信されたネットワーク経路を記憶する。

【００７０】

次に、有利なことに、ホームコントロールネットワークデバイス61は、ICMPルート記録操作も実行し、発見されたルートをホームコントロールネットワークサーバ21にレポートする。ホームコントロールネットワークサーバ21は、そのデータベースに、ホームコントロールネットワークデバイス61から受信されたルートを記憶する。

【００７１】

その後、ホームコントロールネットワークデバイス61は、ホームコントロールネットワークサーバ21に問い合わせを送信することによって、空きサイバースペースの自動判定を実行する。ホームコントロールネットワークサーバ21は、図1および2の例においては、サイバースペース172.17.0.0/24をホームコントロールネットワークデバイス61に返す。

【００７２】

ホームコントロールネットワークデバイス61は、そのサイバースペースをそのイントラネット6のために使用し、それ自体のIPアドレスとして172.17.0.1を取得する。ホームコ

ントロールネットワークデバイス61は、使用することについてホームコントロールネットワークサーバ21に知らせ、サーバが、そのデータベースにその情報を記憶する。

【００７３】

図1および2においては、ホームコントロールネットワークデバイス61は、建物内のデバイスを制御するためのそれ自体のサブネットワークを確立するそれ自体分かれたデバイスとして示されている。ホームコントロールネットワークデバイス61の機能が、十分なプロセッサおよびメモリ容量と、有線データ転送接続かまたは無線データ転送接続かのどちらかによってさまざまな技術的な手段をそれに接続するための接続手段とを有するコンピュータ化されたデバイスまたはハウスエンジニアリング(house engineering)デバイスの一部として組み込まれ得ることは、当業者に明らかである。

【００７４】

ホームコントロールネットワークキー42:

【００７５】

ホームコントロールネットワークキー42のWANポートは、10.0.1.0/24のネットワーク(データ転送ネットワーク3)に接続される。ホームコントロールネットワークキー42は、DHCPサーバ、参照番号31からIPアドレス情報を取得し、ファイアウォールFW2がそのDHCPサーバとして機能する。ホームコントロールネットワークキーは、IPアドレス10.0.1.2を取得する。ホームコントロールネットワークキー42のデフォルトルータ31のアドレスは10.0.1.1であり、DNSサーバ31のアドレスは10.0.1.1であり、これらのアドレスは、DHCPサーバから得られる。

【００７６】

ホームコントロールネットワークキー42は、DNSサーバの助けを借りて、ホームコントロールネットワークサーバ21(HCNS、DNSアドレスhcns.fi)のIPアドレスを突き止めることによって通信を開始する。図1および2の例においては、DNSサーバ10.0.1.1が、ホームコントロールネットワークサーバ21のIPアドレスとして240.1.1.1を与える。

【００７７】

その後、ホームコントロールネットワークキー42は、第1にUDPプロトコル、第2にTCPプロトコルを用いて、インターネットを介してアドレス240.1.1.1のホームコントロールネットワークサーバ21に連絡する。ホームコントロールネットワークキー42は、予め配布された証明書および/またはパスワードによって、ホームコントロールネットワークサーバ21との相互の動作権限を認証する。有利なことに、データ転送接続は、例えば、SSL/TLS暗号化によって暗号化される。ホームコントロールネットワークサーバ21は、着信する接続から、ホームコントロールネットワークキー42のパブリックIPアドレス240.2.1.2を知る。加えて、ホームコントロールネットワークキー42は、ホームコントロールネットワークサーバ21に、そのホームコントロールネットワークキー42自体のアドレスおよびネットワークマスク10.0.1.2/24を知らせる。ホームコントロールネットワークサーバ21は、そのデータベースにこの情報を記憶する。

【００７８】

次に、ホームコントロールネットワークキー42は、traceroute操作を実行し、発見されたネットワーク経路をホームコントロールネットワークサーバ21にレポートし、ホームコントロールネットワークサーバ21がそのデータベースにその情報を記憶する。

【００７９】

有利なことに、ホームコントロールネットワークキー42は、ICMPルート記録操作も実行し、発見されたネットワーク経路をホームコントロールネットワークサーバ21にレポートし、ホームコントロールネットワークサーバ21がそのデータベースにその情報を記憶する。

【００８０】

ホームコントロールネットワークサーバ21は、受信されたルート情報を調べ、重複がある場合、それらをホームコントロールネットワークキー42にレポートし、ホームコントロールネットワークキー42が、必要に応じて、空きサイバースペースの自動判定を改めて実

行する。
【００８１】
ホームコントロールネットワークキーとしてのデータ処理デバイス41c:
【００８２】
図2による実施形態1Bにおいては、ホームコントロールネットワークキー42が、ユーザのデータ処理デバイス41cによって置き換えられており、ホームコントロールネットワークキーの機能を含むコンピュータプログラムが、ホームコントロールネットワークキーの第2の実施形態によるホームコントロールネットワークキー42bから記憶されている(参照符号42e)。有利なことに、前記ホームコントロールネットワークキー42bは、いわゆるUSBスティックである可能性がある。図2の実施形態においては、ホームコントロールネットワークキー42の上述の機能が、USBスティック42bからユーザのデータ処理デバイス41cにインストールされたコンピュータプログラムによって実行される。
【００８３】
遠隔制御システム1Aを使用したアクチュエータの制御の例。
【００８４】
何らかのデバイスが、接続されるべきそのデバイスを永続的な接続かまたは無線かのどちらかでホームコントロールネットワークデバイス61のイントラネットインターフェースに接続することによって遠隔制御システム1Aに接続される。
【００８５】
例えば、暖房制御ウェブサーバ63(HCWS)が、ハウスコントロールイントラネットネットワーク6に接続される。この例においては、暖房制御ウェブサーバ63は、接続された後、DHCPサービスによってそのIP設定を取得する。暖房制御ウェブサーバは、ホームコントロールネットワークデバイス61から、その暖房制御ウェブサーバ自体のアドレスとして172.17.0.4を取得し、デフォルトルータのアドレスとして172.17.0.1を取得し、DNSサーバのアドレスとして172.17.0.1を取得する。さらに、暖房制御ウェブサーバは、DNSサーバから、図1の例においてはhcws.hcnd.localをその名前として取得する。
【００８６】
ホームコントロールネットワークデバイス61は、そのローカルデータベースに、そのホームコントロールネットワークデバイス61が暖房制御ウェブサーバ63に与えるDHCP情報を記憶する。
【００８７】
ホームコントロールネットワークキー42は、ホームコントロールネットワークデバイス61とペアになるように予め決められる。このようにして、ハウスコントロールイントラネット6と、ホームコントロールネットワークキー42が接続されるイーサネット(登録商標)ネットワーク3との間に、直接的なデータ転送接続を確立することができる。
【００８８】
ホームコントロールネットワークキー42は、ペア形成プロセスを開始する。ホームコントロールネットワークキー42は、有利なことにUDPプロトコルを使用して、ホームコントロールネットワークデバイス61へのデータ転送接続を確立したいことをホームコントロールネットワークサーバ21に知らせる。ホームコントロールネットワークサーバ21は、要求されたデータ転送接続が以下のポート番号を用いて確立されるべきであると決定する。
- ホームコントロールネットワークキー: UDP送信元ポート10500、UDP送信先ポート10501、送信先IPアドレス240.1.1.2
- ホームコントロールネットワークデバイス: UDP送信元ポート10501、UDP送信先ポート10500、送信先IPアドレス240.2.1.2
【００８９】
ホームコントロールネットワークサーバ21は、この情報を、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61にレポートする。
【００９０】
その後、ホームコントロールネットワークキー42は、送信先ポート10501への送信元ポ

ート10500を用いて、UDPパケットをアドレス240.1.1.2に送信する。送信されたパケットは、発信されるトラフィックが厳しく制限されていないので、NAT機能を含むファイアウォールFW2を通り抜ける。FW2ファイアウォール31は、その後X秒間、連絡先情報10.0.0.2、240.1.1.2、10500、および10501とともに、UDPパケットを接続として記憶している。

【００９１】

UDPパケットはFW1ファイアウォール51に到着し、FW1ファイアウォール51は着信するトラフィックを認めず、パケットを破棄する。パケットは、アドレス10.0.0.2に到着しない。

【００９２】

ホームコントロールネットワークデバイス61は、送信先ポート10500への送信元ポート10501を用いて、UDPパケットをアドレス240.2.1.2に送信する。送信されたUDPパケットは、発信されるトラフィックが制限されていないので、FW1 NATファイアウォール51を通り抜ける。FW1ファイアウォール51は、その後X秒間、連絡先情報10.0.0.2、240.2.1.2、10501、および10500とともに、UDPパケットを接続として記憶している。

【００９３】

UDPパケットは、FW2ファイアウォール31に到着する。FW2ファイアウォール31は、IPアドレス10.0.1.2が送信元ポート10500および送信先ポート10501を用いてアドレス240.1.1.2へのUDP接続を確立したことを記憶している。UDPパケットが、送信元ポート10501を用いて送信先ポート10500に前記送信元アドレス240.2.1.2から到着するので、FW2ファイアウォール31は、そのパケットを、デバイス10.0.1.2によって確立された接続に関連する返ってくる通信であると解釈する。その後、ファイアウォールFW2は、アドレス変更操作を実行する。ファイアウォールFW2は、UDPパケットの送信先アドレスを10.0.1.2に変更する。その後、FW2ファイアウォール31は、UDPパケットをアドレス10.0.1.2にルーティングする。以降、ホームコントロールネットワークキー42は、ホームコントロールネットワークデバイス61からメッセージを受信する。この時点で、ホームコントロールネットワークデバイス61からホームコントロールネットワークキー42への片方向のデータ転送接続が存在する。

【００９４】

次に、ホームコントロールネットワークキー42は、送信先ポート10501への送信元ポート10500を用いて、UDPパケットをアドレス240.1.1.2に送信する。UDPパケットは、FW1ファイアウォール51に到着する。FW1ファイアウォール51は、アドレス10.0.0.2が、送信元ポート10501および送信先ポート10500を用いて、アドレス240.2.1.2へのUDP接続を確立したことを記憶している。パケットが、送信元ポート10500を用いて送信先ポート10501に送信元アドレス240.2.1.2から到着するので、FW2ファイアウォール51は、受信されたUDPパケットを、デバイス10.0.0.2によって確立された接続に関連する返ってくる通信であると解釈する。FW1ファイアウォール51は、アドレスの変更を実行し、すなわち、パケットの送信先アドレスを10.0.0.2に変更する。その後、FW1ファイアウォール51は、パケットをアドレス10.0.0.2にルーティングする。

【００９５】

この時点で、ホームコントロールネットワークキー42とホームコントロールネットワークデバイス61との間に双方向のUDP接続が存在する。これらのデバイスは、互いに双方向通信できる。有利なことに、ホームコントロールネットワークデバイス61およびホームコントロールネットワークキー42は、例えば、OpenVPNソフトウェアを使用してそれらの間にデータリンク層レベルのVPNトンネルを形成する。

【００９６】

ホームコントロールネットワークデバイス61は、生成されたVPNトンネル55を、そのホームコントロールネットワークデバイス61が管理するハウスコントロール遠隔ネットワーク172.17.0.0/24、参照番号6にブリッジする。同じように、ホームコントロールネットワークキー42は、データリンク層レベルでネットワーク172.17.0.0/24でイントラネットのインターフェースを提供することができるように、生成されたVPNトンネル55をそのホー

ムコントロールネットワークキー42のLANポートにブリッジする。これらの動作の後、ハウスコントロール遠隔ネットワーク4およびハウスコントロールイントラネット6は、インターネット2を介してプライベートVPNネットワークを形成する。

【００９７】

今や、クライアントデバイス41aが、ホームコントロールネットワークキー42のイントラネットインターフェースにイーサネット(登録商標)を介して接続可能であり、このインターフェースは、例えば、LANインターフェースである可能性がある。接続された後、クライアントデバイス41aは、そのIP設定を、DHCPプロトコルを使用することによってホームコントロールネットワークデバイス61から取得する。クライアントデバイス41aまたは41cによって送信されたDHCP問い合わせは、ホームコントロールネットワークキー42のLANポートに到着し、そのポートは、VPNトンネル55にブリッジされている。ホームコントロールネットワークキー42は、クライアントデバイス41aまたは41cによって形成されたイーサネット(登録商標)パケットをVPNトンネル55にそのまま送信する。クライアントデバイス41aまたは41cによって送信されたDHCPパケットは、VPNトンネル55を伝わってホームコントロールネットワークデバイス61に到着する。

【００９８】

ホームコントロールネットワークデバイス61は、DHCPサーバを備えており、そのDHCPサーバが、返信メッセージで、IPアドレス172.17.0.7/24、デフォルトルータ172.17.0.1、およびDNSサーバ172.17.0.1と応答する。それに対応して、ホームコントロールネットワークデバイス61の返信メッセージは、VPNトンネル55を伝わってホームコントロールネットワークキー42に到着し、ホームコントロールネットワークキー42が、そのLANネットワークインターフェースに向けてそのパケットを送信する。LANネットワークインターフェースを通じて、クライアントデバイス41aまたは41cは、DHCPの返信パケットを受信し、IP返信パケットに含まれる設定を使用する。この時点で、クライアントデバイスのIPアドレスは172.17.0.7/24であり、デフォルトルータのIPアドレスは172.17.0.1であり、DNSサーバのIPアドレスは172.17.0.1である。

【００９９】

クライアントデバイス41aは今や論理的にVPNネットワーク172.17.0.0/24の一部であり、まるで172.17.0.0/24のネットワーク(ハウスコントロールイントラネット6)に物理的に直接接続されているかのように、デバイス172.17.0.4とイーサネット(登録商標)レベルで直接通信することができる。しかし、接続速度および遅延などのVPNトンネル55およびインターネット接続の技術的な制限が、通信するときに考慮されなくてはならない。

【０１００】

遠隔制御されるべきデバイスが、永続的かまたは無線かのどちらかで、ホームコントロールネットワークデバイス61のLANインターフェースに接続される。図1および2の例においては、接続されるべきデバイスは、空調制御65、暖房制御63、監視カメラ64、および照明制御62である。遠隔制御されるべきデバイスのウェブサーバは、有利なことにホームコントロールネットワークデバイスに含まれるDHCPサーバからそれらのデバイスのIPアドレスを受信する。

【０１０１】

ホームコントロールネットワークデバイス61は、所定の方法で、そのホームコントロールネットワークデバイス61が与えるIPアドレスに名前を付ける。図1および2の例において、IPアドレス172.17.0.4は「HCND1」であり、これは暖房制御である。それに対応して、IPアドレス172.17.0.3は「HCND2」であり、これは監視カメラである。

【０１０２】

今や、クライアントデバイス41のユーザは、図1に示された遠隔制御されるべきデバイス62、63、64、および65とイーサネット(登録商標)レベルで直接通信することができる。通信は、遠隔制御されるべきデバイスにサービスを提供するハウスコントロールイントラネットネットワーク172.17.0.0/24にクライアントデバイス41aが物理的に直接接続されたとした場合に使用されるであろう方法とは異ならない。

【０１０３】
本発明による遠隔制御システム1Aを利用するとき、クライアントデバイス41aのユーザは、ブラウザで、アドレスとして、例えばhttp://hcnd1と入力する。クライアントデバイスのブラウザは、名前「HCND1」に関して(アドレス172.17.0.1から)ホームコントロールネットワークデバイス61にDNS問い合わせを行う。ホームコントロールネットワークデバイス61は、クライアントデバイス41aに、HCND1のIPアドレス172.17.0.4とともに名前を返す。有利なことに、ユーザのクライアントデバイス41aのブラウザは、HTTPを用いて、暖房制御ウェブサーバ172.17.0.4からのページhttp://HCND1を開く。この時点で、ユーザは、暖房制御を制御する暖房制御ウェブサーバ63への直接的な管理接続を有する。
【０１０４】
クライアントデバイス41aのユーザは、プライマリネーム(primary name)「HCND」に関するアドレス検索を実行することもできる。ホームコントロールネットワークデバイス61は、それ自体のIPアドレス172.17.0.1で問い合わせに応答し、ユーザのクライアントデバイス41aのブラウザで見られるべきインデックスページを提供する。インデックスページで、ユーザは、ホームコントロールネットワークデバイス61のLANインターフェースに接続されたすべてのリソースをリスト形式で見る。図1および2の例においては、以下のリストがブラウザで見られる。

hcnd1 172.17.0.4
hcnd2 172.17.0.3
hcnd3 172.17.0.2
hcnd4 172.17.0.5

【０１０５】
インデックスページで、クライアントデバイスのユーザは、表示されたオブジェクト、例えば「HCND1」の名前を名前「暖房制御」に変更し、「HCND2」の名前を名前「監視カメラ」に変更することができる。ホームコントロールネットワークデバイスは、問題のIPアドレスに関する名前の変更を自動的に記憶する。以降、クライアントデバイス41aのユーザは、例えば、ブラウザの行に「暖房制御」とだけ入力することによって暖房制御に連絡することができる。
【０１０６】
図1および2に関連して、クライアントデバイス41a、41bまたは41cおよび建物内の遠隔制御されるべきデバイス62～65が本発明の遠隔制御システムにおいて情報および制御命令をどのようにして交換させられる可能性があるのかを示すための例が使用された。
【０１０７】
図1による実施形態においては、有利なことに、ホームコントロールネットワークキー42およびホームコントロールネットワークデバイス61のペアが、製造に関連して決定される。
【０１０８】
図2による実施形態においては、ホームコントロールネットワークキー42bおよびホームコントロールネットワークデバイス61のペア形成は、製造に関連してか、または最終的な使用対象においてかのどちらかで決定され得る。ペア形成の決定が最終的な使用対象において行われる場合、ホームコントロールネットワークキー42bは、図2による実施形態において、ホームコントロールネットワークデバイス61に一時的に接続される。有利なことに、接続は、デバイスのUSBポートによってか、または無線ネットワークを介してかのどちらかで実施される。
【０１０９】
結合を介して、ホームコントロールネットワークキー42bおよびホームコントロールネットワークデバイス61は、そのデバイスのペアの識別コードを受信し、それ自体の識別コードをそのデバイスのペアに送信することができる。その後、これらの2つのデバイスは、お互いとだけデータ転送接続を確立することができる。
【０１１０】

有利なことに、ユーザのユーザ端末41cへのホームコントロールネットワークキーのコンピュータプログラムの転送は、以下のように実施される。

【０１１１】

ホームコントロールネットワークキー42bがその接続によってデータ処理デバイス41cにしばらくの間接続されるとき、ホームコントロールネットワークキー42bに含まれるコンピュータプログラムが、その個々の識別コードとともに、ユーザのデータ処理デバイス41cにインストールされる(参照符号42e)。インストールに関連して、データ処理デバイス41cのユーザは、デバイスおよび/またはプログラムの保護機能を利用したいかどうかを尋ねられる。保護機能を作動させることが望ましい場合、この場合、ホームコントロールネットワークキーのインストールプログラムは、ユーザがそのユーザのパスワードをユーザのデータ処理デバイス41cかもしくはインストールされたプログラムかのどちらかにのみ与えるか、または必要に応じて両方に与えることを要求する。

【０１１２】

ホームコントロールネットワークキーは、そのプログラム、個々の識別コード、およびパスワードとともに、例えば、厳重に保護された内部ネットワークサーバに必要に応じて記憶される可能性もあり、その内部ネットワークサーバから新しいホームコントロールネットワークキーに、必要なときに(例えば、元のキーデバイスが壊れるかまたはなくなった場合に)戻される可能性がある。

【０１１３】

本発明の有利な実施形態においては、ホームコントロールネットワークキー42bに含まれるプログラムが、その識別コードとともに、いくつかのデータ処理デバイス41cに記憶される可能性もあり、したがって、それらのデータ処理デバイス41cは、第1のデータ処理デバイスと並列に機能する可能性がある。

【０１１４】

本発明の有利な実施形態においては、ホームコントロールネットワークキー42bに含まれるコンピュータプログラムが、例えば、インターネット上のサーバにある可能性もあり、そのサーバから取得される可能性がある。この有利な実施形態においては、物理的なホームコントロールネットワークキー42b自体は、デバイスのペアを特定するために必要とされる識別コードのみを含む可能性がある。

【０１１５】

図3は、ホームコントロールネットワークキー42または42bとホームコントロールネットワークデバイス61とが一緒にペアにされた後の上述の動作を流れ図として示す。

【０１１６】

ステップ300において、ホームコントロールネットワークデバイス61が、ハウスイントラネットネットワーク5に接続され、ホームコントロールネットワークキー42、またはホームコントロールネットワークキーをシミュレートするデータ処理デバイス41cが、イントラネットネットワーク3に接続される。建物内の遠隔制御されるべきすべてのデバイスが、永続的な接続かまたは無線接続かのどちらかでホームコントロールネットワークデバイス61に接続される。

【０１１７】

ステップ301において、ホームコントロールネットワークデバイス61およびホームコントロールネットワークキー42または41cが、それらのネットワーク経路を判定する。ステップ302において、ホームコントロールネットワークデバイス61とホームコントロールネットワークキー42とが、それらの判定されたネットワーク経路をホームコントロールネットワークサーバ21に記憶する。

【０１１８】

ステップ303において、遠隔制御で利用されるべき本発明によるデバイス42または41cおよび61が、それらのデバイスのペアがホームコントロールネットワークサーバ21に登録されているという情報、または登録が見つからないという情報を受信する。デバイスのペアに属する本発明によるデバイス42/41cまたは61のうちの1つが登録されていない場合、遠

隔制御システム1Aまたは1Bは、規定された遅延312の後、ホームコントロールネットワークサーバ接続のリスニングステップ313に移る。

【０１１９】

接続の確立の初めに、ホームコントロールネットワークキー42/41cとホームコントロールネットワークデバイス61との両方が、ステップ304において、ホームコントロールネットワークサーバ21からの相手のネットワーク経路を要求する。ステップ305において、ホームコントロールネットワークサーバ21が、それが許可されたデバイスのペアの問いであることを調べ、調べた後、ネットワーク経路を両方のデバイスに送信する。その後、ホームコントロールネットワークサーバ21は、デバイス42/41cと61との両方への接続を解放し、したがって、もはや、形成されているVPNトンネル55の一部ではなくなる。

【０１２０】

ステップ306において、ホームコントロールネットワークキー42/41cおよびホームコントロールネットワークデバイス61が、それらの間のVPNトンネル55を形成する。

【０１２１】

ステップ307において、ユーザのクライアントデバイス41aまたは41cと建物内の対象のデバイス62～65との両方が、確立されたVPNネットワークに接続される。図1の実施形態においては、ユーザのクライアントデバイス41aが、ホームコントロールネットワークキー42によってVPNネットワークに接続される。図2の実施形態においては、ユーザのデータ処理デバイス41c自体が、VPNネットワークのエンドポイントのうちの1つである。対象で遠隔制御されるべきデバイス62～65は、ホームコントロールネットワークデバイス61によってVPNネットワークに接続される。

【０１２２】

ステップ308において、ユーザのクライアントデバイス41aまたは41cと建物内で制御されるべきデバイス62～65とが同じVPNネットワークの一部であり、それによって、それらが互いに情報を交換する。遠隔制御システムで規定された遅延の後、ステップ309は、クライアントデバイス41aまたは41cと対象のデバイス62～65との間のデータ転送接続がまだアクティブであるかどうかを調べることからなる。データ転送接続がアクティブである場合、プロセスはステップ308に戻り、データ転送が継続することを許される。

【０１２３】

ステップ309において、VPN接続がもはやアクティブでないことが判明する場合、ステップ310において、接続を確立する可能な新たな試みに関する決定が行われる。接続を確立する新たな試みを行うと決定される場合、プロセスはステップ301に戻る。この代替的方法において、プロセスは、有利なことに、本発明による接続確立プロセス自体が正常に更新され得るように、VPN接続を解放するための必要な手順も含む。接続の確立は、所定の回数にしたがって試みられる。

【０１２４】

ステップ310において、所定の回数の接続を確立する試みが行われたか、または何らかのその他の理由でVPN接続を確立することが望ましくないために、VPN接続を確立する新たな試みがもはや行われないと決定される場合、プロセスはステップ311に移る。ステップ311において、使用されたVPNデータ転送ネットワークが解放される。

【０１２５】

VPNデータ転送ネットワークが解放された後、遠隔制御システム1Aまたは1Bで利用されるプロセスで所定の遅延312が起こる。遅延312の後、プロセスは、ホームコントロールネットワークサーバのリスニング機能313に移る。そこで、通電(current-carrying)ホームコントロールネットワークデバイス61が、ネットワークを介してホームコントロールネットワークサーバ21に連絡要求を送信する。

【０１２６】

ホームコントロールネットワークデバイス61は、ホームコントロールネットワークサーバ21へのネットワーク接続が確立されるまで、プロセス、ステップ314を繰り返す。

【０１２７】

ホームコントロールネットワークサーバ21へのデータ転送接続が確立されているとき、ステップ314において、VPN接続を確立するプロセスに移ることについての決定がなされ、それによってプロセスはステップ301に戻る。

【０１２８】

上述のプロセスのステップのすべては、好適な専用プロセッサまたは汎用プロセッサで実行されるプログラム命令で実装される。プログラム命令は、メモリなどの、ホームコントロールネットワークデバイス61およびホームコントロールネットワークキー42によって利用されるストレージ媒体に記憶され、そのストレージ媒体から、プロセッサがそれらのプログラム命令を取得し、実施することができる。例えば、コンピュータ可読媒体が表すものには、プログラム可能なUSBフラッシュメモリ、ロジックアレイ(FPLA)、特定用途向け集積回路(ASIC)、および信号プロセッサ(DSP)などの特別なコンポーネントも含まれる可能性がある。

【０１２９】

図4は、本発明によるホームコントロールネットワークデバイス61の機能の主要な部分を示す。ホームコントロールネットワークデバイス61は、電源621を有する。電源621は、蓄電池、またはコンセントの電流に基づく電源である可能性がある。ホームコントロールネットワークデバイスのすべての電気的なコンポーネントは、電源621からそれらの動作電圧を得る。

【０１３０】

ホームコントロールネットワークデバイス61は、1つまたは複数のプロセッサ622を有する。プロセッサまたはプロセッサ手段は、算術論理演算ユニット、一群の異なるレジスタ、および制御回路を含む可能性がある。コンピュータ可読情報またはプログラムまたはユーザの情報が記憶され得るメモリユニットまたはメモリ手段などのデータ記憶構成623が、プロセッサ手段に接続されている。典型的には、メモリ手段623は、読み取り機能と書き込み機能との両方を認めるメモリユニット(ランダムアクセスメモリ、RAM)と、データが読み取りだけ可能である不揮発性メモリを含むメモリユニット(読み出し専用メモリ、ROM)とを含む。有利なことに、デバイスの識別情報、デバイスの現在のネットワーク経路、デバイスのペアとして機能するホームコントロールネットワークキー42の識別情報、およびホームコントロールネットワークデバイス61の動作に必要なすべてのプログラムは、メモリ手段に記憶される。

【０１３１】

ホームコントロールネットワークデバイス61のメモリに記憶されるプログラムのいくつかの例は、オペレーティングシステム(例えば、Linux(登録商標))、TCP/IPプログラム、VPNプログラム(例えば、OpenVPN)、DHCPクライアントデバイス/サーバプログラム(例えば、ISC DHCP)、DNSサーバプログラム(例えば、dnsmasq)、データベースプログラム(例えば、SQLite)、遠隔制御プログラム(例えば、OpenSSH)、証明書管理/確認プログラム(例えば、GPG)、およびユーザインターフェースライブラリ(例えば、LuCI)である。

【０１３２】

ホームコントロールネットワークデバイス61は、情報を受信または送信するための入力/出力または入力/出力手段624、625、626、および627を含むインターフェース要素も含む。入力手段によって受信された情報は、ホームコントロールネットワークデバイス61のプロセッサ手段622によって処理されるように転送される。ホームコントロールネットワークデバイスのインターフェース要素は、データ転送ネットワークかまたは外部のデータ処理デバイスかのどちらかに情報を転送する。有利なことに、ホームコントロールネットワークデバイス61のインターフェース要素は、WANポート624、1つまたは複数のLANポート625、アンテナポート626、およびUSBポート627である。有利なことに、ホームコントロールネットワークデバイス61およびホームコントロールネットワークキー42または41cのペア形成は、例えば、USBポート627を介して行われ得る。

【０１３３】

ホームコントロールネットワークデバイス61の機能が、十分なプロセッサおよびメモリ

容量と、有線データ転送接続かまたは無線データ転送接続かのどちらかによってさまざまな技術的な手段をそれに接続するための接続手段とを有するコンピュータ化されたデバイスまたはハウスエンジニアリングデバイスの一部として組み込まれ得ることは、当業者に明らかである。ホームコントロールネットワークデバイスの機能が組み込まれるコンピュータ化されたデバイスは、何らかのデータ転送ネットワーク5に接続され、データ転送ネットワーク5からパブリックインターネットにアクセスすることができる。

【０１３４】

図5aは、本発明によるホームコントロールネットワークキー42の機能の主要な部分を示す。ホームコントロールネットワークデバイス42は、電源421を有する。電源421は、蓄電池、またはコンセントの電流に基づく電源である可能性がある。ホームコントロールネットワークデバイスのすべての電気的なコンポーネントは、電源421からそれらの動作電圧を得る。

【０１３５】

ホームコントロールネットワークキー42は、1つまたは複数のプロセッサ422を含み得る。プロセッサまたはプロセッサ手段は、算術論理演算ユニット、一群の異なるレジスタ、および制御回路を含む可能性がある。コンピュータ可読情報またはプログラムまたはユーザの情報が記憶され得るメモリユニットまたはメモリ手段などのデータ記憶構成423が、プロセッサ手段に接続されている。典型的には、メモリ手段423は、読み取り機能と書き込み機能との両方を認めるメモリユニット(ランダムアクセスメモリ、RAM)と、データが読み取りだけ可能である不揮発性メモリを含むメモリユニット(読み出し専用メモリ、ROM)とを含む。有利なことに、デバイスの識別情報、デバイスの現在のネットワーク経路、デバイスのペアとして機能するホームコントロールネットワークデバイスの識別情報、およびホームコントロールネットワークキー42の動作に必要なすべてのプログラムは、メモリ手段に記憶される。

【０１３６】

ホームコントロールネットワークキー42のメモリに記憶されるプログラムのいくつかの例は、オペレーティングシステム(例えば、Linux(登録商標))、TCP/IPプログラム、VPNプログラム(例えば、OpenVPN)、DHCPサーバ/クライアントデバイスプログラム(例えば、ISC DHCP)、DNSサーバプログラム(例えば、dnsmasq)、データベースプログラム(例えば、SQLite)、遠隔制御プログラム(例えば、OpenSSH)、証明書管理/確認プログラム(例えば、GPG)、およびユーザインターフェースライブラリ(例えば、LuCI)である。

【０１３７】

ホームコントロールネットワークキー42は、情報を受信または送信するための入力/出力または入力/出力手段424、425および426を含むインターフェース要素も含む。入力手段によって受信された情報は、ホームコントロールネットワークキー42のプロセッサ手段422によって処理されるように転送される。ホームコントロールネットワークデバイスのインターフェース要素は、データ転送ネットワークかまたは外部のデータ処理デバイスかのどちらかに情報を転送する。有利なことに、ホームコントロールネットワークデバイス42のインターフェース要素は、WANポート424、LANポート425、USBポート426、およびアンテナポート427である。

【０１３８】

図5bは、本発明の第2の実施形態によるホームコントロールネットワークキー42bの機能の主要な部分を示す。この実施形態によるホームコントロールネットワークキー41cは、1つまたは複数のプロセッサ422を含み得る。プロセッサまたはプロセッサ手段は、算術論理演算ユニット、一群の異なるレジスタ、および制御回路を含む可能性がある。コンピュータ可読情報またはプログラムまたはユーザの情報が記憶され得るメモリユニットまたはメモリ手段などのデータ記憶構成423が、プロセッサ手段に接続されている。典型的には、メモリ手段423は、読み取り機能と書き込み機能との両方を認めるメモリユニット(ランダムアクセスメモリ、RAM)と、データが読み取りだけ可能である不揮発性メモリを含むメモリユニット(読み出し専用メモリ、ROM)とを含む。有利なことに、ホームコントロール

ネットワークキー42bの識別情報、その現在のネットワーク経路、そのデバイスのペアとして機能するホームコントロールネットワークデバイス61の識別情報、ならびにホームコントロールネットワークキー41cの動作に必要なすべてのプログラムは、メモリ手段に記憶される。

【０１３９】

ホームコントロールネットワークキー42bのメモリに記憶されるプログラムのいくつかの例は、オペレーティングシステム(例えば、Linux(登録商標))、TCP/IPプログラム、VPNプログラム(例えば、OpenVPN)、DHCPクライアントデバイスプログラム(例えば、ISC DHCP)、データベースプログラム(例えば、SQLite)、証明書管理/確認プログラム(例えば、GPG)、およびユーザインターフェースライブラリ(例えば、LuCI)である。

【０１４０】

ホームコントロールネットワークキー42bは、情報を受信または送信するための入力/出力または入力/出力手段426を含むインターフェース要素も含む。入力手段によって受信された情報は、ホームコントロールネットワークキー42bのプロセッサ手段422によって処理されるように転送される。有利なことに、ホームコントロールネットワークデバイスのインターフェース要素は、ホームコントロールネットワークキーのメモリ423から外部データ処理デバイス41cかまたはホームコントロールネットワークデバイス61かのどちらかに情報を転送するために使用される。それに対応して、情報または命令が、例えば、ホームコントロールネットワークキー42bが接続されるデータ処理デバイスからインターフェース要素を介して受信され得る。

【０１４１】

それらのアクセス権限のレベルに関して、少なくとも2つのレベルの上述のホームコントロールネットワークキー42または42b、例えば、管理者レベルキーデバイスおよび基本ユーザレベルキーデバイスが存在する。より高いアクセス権限のレベルのキーデバイスのユーザ/所有者(例えば、管理者)は、(基本ユーザなどの)より低いレベルのホームコントロールネットワークキーのユーザのすべての制御対象に対する制御権限を有する。一方、より低いレベルのキーデバイスのアクセス権限のレベルの所有者は、その所有者自身の対象以外のいかなるより高いアクセス権限のレベルの制御対象にもアクセスすることができない。

【０１４２】

図6は、本発明によるホームコントロールネットワークサーバ21の機能の主要な部分を示す。ホームコントロールネットワークサーバ21は、電源211を含む。電源211は、蓄電池、またはコンセントの電流に基づく電源である可能性がある。ホームコントロールネットワークサーバ21のすべての電気的なコンポーネントは、電源211からそれらの動作電圧を得る。

【０１４３】

ホームコントロールネットワークサーバ21は、1つまたは複数のプロセッサ212を有する。プロセッサまたはプロセッサ手段は、算術論理演算ユニット、一群の異なるレジスタ、および制御回路を含む可能性がある。コンピュータ可読情報またはプログラムまたはユーザの情報が記憶され得るメモリユニットまたはメモリ手段などのデータ記憶構成213が、プロセッサ手段に接続されている。典型的には、メモリ手段213は、読み取り機能と書き込み機能との両方を認めるメモリユニット(ランダムアクセスメモリ、RAM)と、データが読み取りだけ可能である不揮発性メモリを含むメモリユニット(読み出し専用メモリ、ROM)とを含む。有利なことに、遠隔制御システムのデバイスのペアの識別情報、それぞれのデバイスのペアの現在のネットワーク経路、およびデバイスのペアの間で確立されるべきVPNデータ転送接続を確立するために必要なすべてのプログラムは、メモリ手段に記憶される。

【０１４４】

ホームコントロールネットワークサーバ21のメモリに記憶されるプログラムのいくつかの例は、オペレーティングシステム(例えば、Linux(登録商標))、TCP/IPプログラム、DHC

Pサーバ/クライアントデバイスプログラム(例えば、ISC DHCP)、DNSサーバプログラム(例えば、bind)、データベースプログラム(例えば、SQLite)、証明書管理/確認プログラム(例えば、GPG)、およびユーザインターフェースライブラリ(例えば、LuCI)である。

【０１４５】

ホームコントロールネットワークサーバ21は、情報を受信または送信するための入力/出力または入力/出力手段214および215を含むインターフェース要素も含む。入力手段によって受信された情報は、ホームコントロールネットワークサーバ21のプロセッサ手段212によって処理されるように転送される。ホームコントロールネットワークサーバ21のインターフェース要素は、データ転送ネットワークかまたは外部のデータ処理デバイスかのどちらかに情報を転送する。有利なことに、ホームコントロールネットワークサーバ21のインターフェース要素は、WANポート214および1つまたは複数のLANポート215である。

【０１４６】

有利なことに、ホームコントロールネットワークサーバ21は、サーバ21のユーザから情報を受信するための手段を含むユーザインターフェース(図6に示されていない)も含む。ユーザインターフェースは、キーボード、タッチスクリーン、マイクロホン、およびスピーカを含み得る。

【０１４７】

本発明による遠隔制御方法および遠隔制御システムの一部の有利な実施形態が、上で説明された。本発明は、上述のソリューションに限定されず、本発明の概念は、特許請求の範囲内で多くの方法で適用され得る。

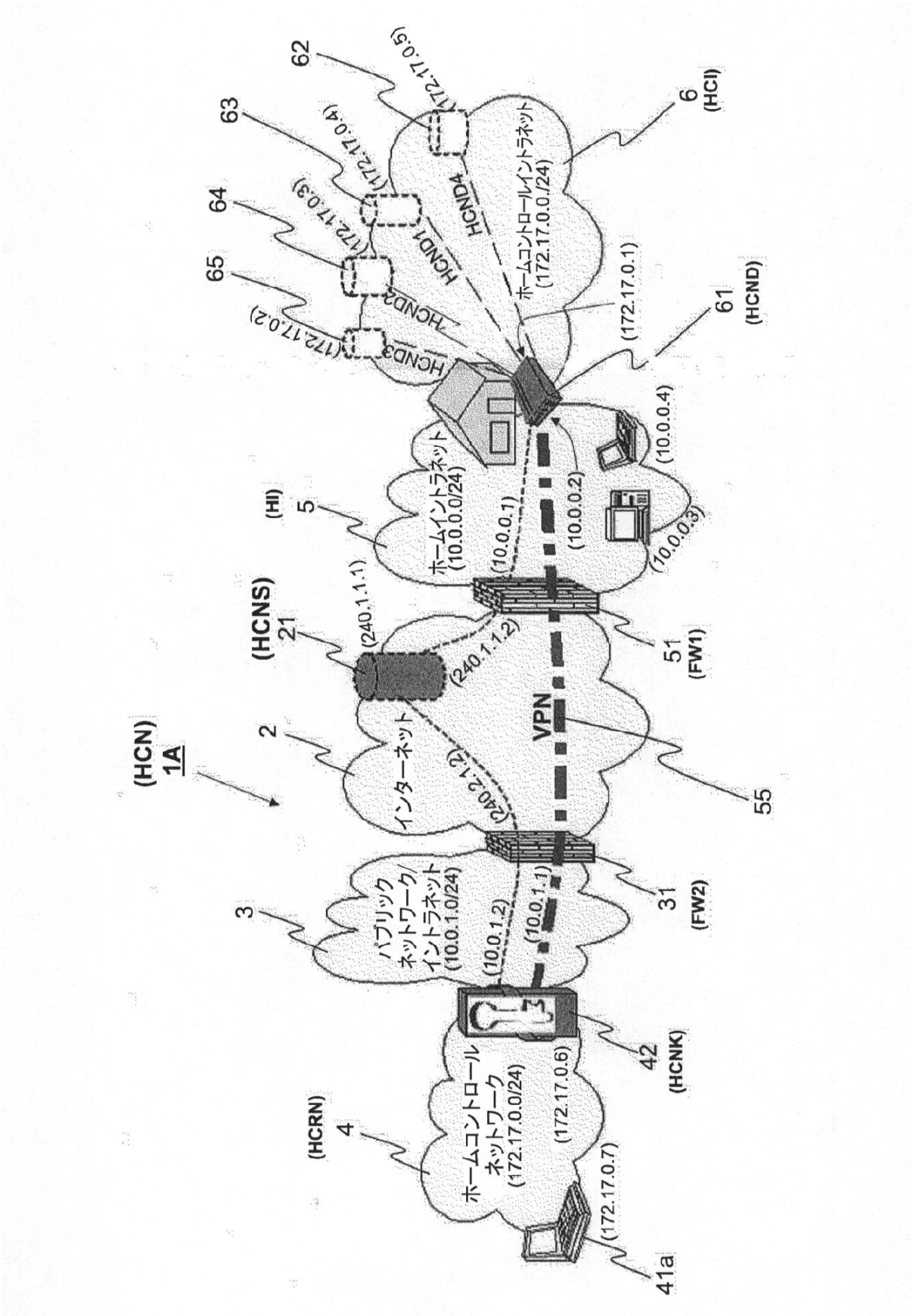
【符号の説明】

【０１４８】

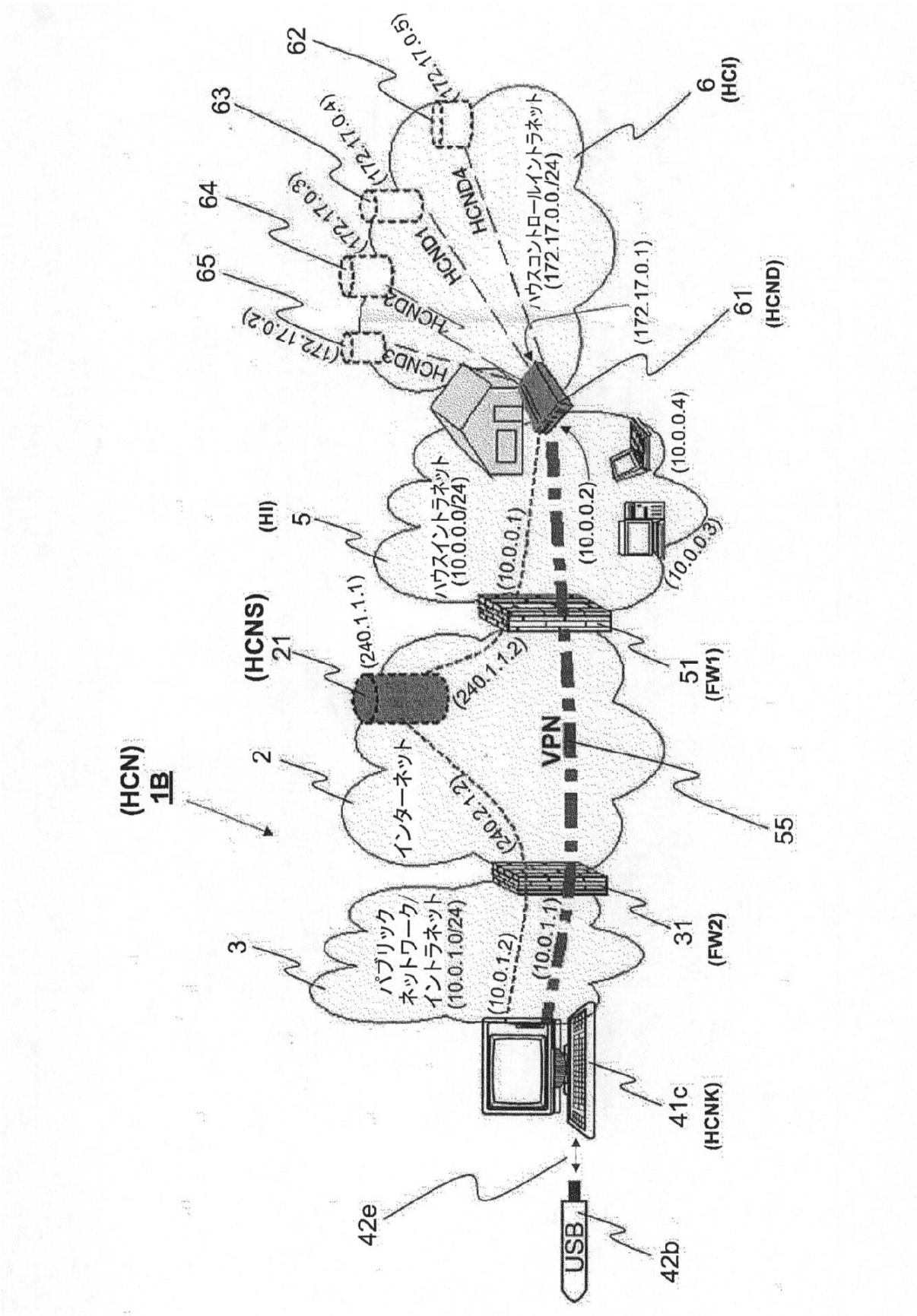
1A 遠隔制御システム
1B 遠隔制御システム
2 インターネット
3 パブリックネットワーク、イントラネット
4 第1のデータ転送ネットワーク、ハウスコントロール遠隔ネットワーク
5 ハウスイントラネット
6 第2のデータ転送ネットワーク、ハウスコントロールイントラネット
21 ホームコントロールネットワークサーバ
31 ファイアウォール、デフォルトルータ、DNSサーバ
41a クライアントデバイス、データ処理デバイス
41b クライアントデバイス、データ処理デバイス
41c クライアントデバイス、データ処理デバイス
42 ホームコントロールネットワークキー
42b ホームコントロールネットワークキー
51 ネットワーク端末、ファイアウォール
55 データ転送接続、VPNトンネル
61 ホームコントロールネットワークデバイス
62 アクチュエータ、デバイス、サーバ、照明制御ウェブサーバ
63 アクチュエータ、デバイス、サーバ、暖房制御ウェブサーバ
64 アクチュエータ、デバイス、サーバ、監視カメラウェブサーバ
65 アクチュエータ、デバイス、サーバ、空調ウェブサーバ
211 電源
212 プロセッサ
213 データ記憶構成
214 入力/出力手段、WANポート
215 入力/出力手段、LANポート
421 電源
422 プロセッサ

423 データ記憶構成
424 入力/出力手段、WANポート
425 入力/出力手段、LANポート
426 入力/出力手段、USBポート
427 入力/出力手段、アンテナポート
621 電源
622 プロセッサ
623 データ記憶構成
624 入力/出力手段、WANポート
625 入力/出力手段、LANポート
626 入力/出力手段、アンテナポート
627 入力/出力手段、USBポート

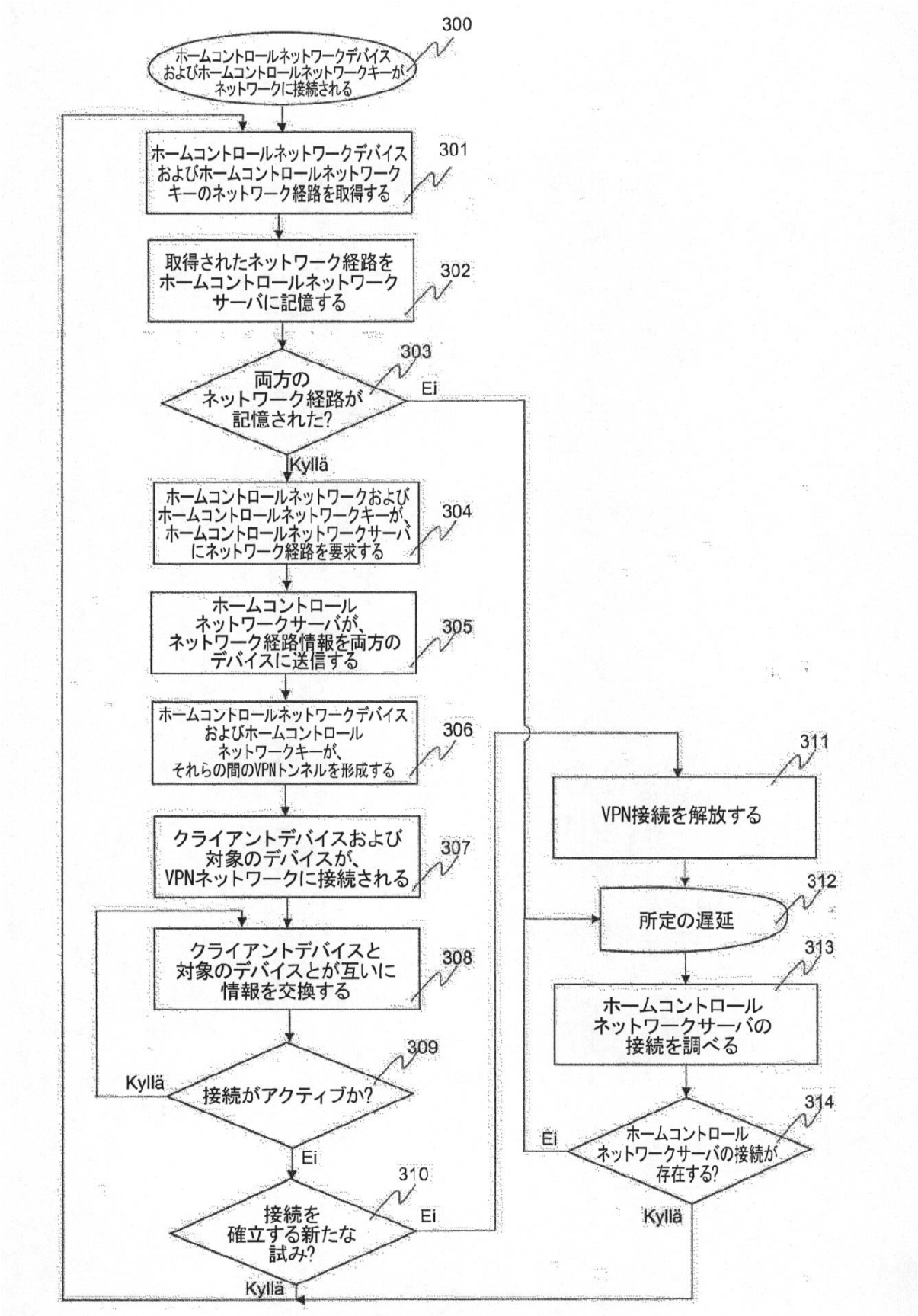
【図１】


(HCN)
1A
2
インターネット
(240.1.1.1)
(240.1.1.2)
(240.2.1.2)
(HCNS)
21
VPN
55
3
パブリック
ネットワーク/
イントラネット
(10.0.1.0/24)
(10.0.1.2)
(10.0.1.1)
31
(FW2)
(HCRN)
4
ホームコントロール
ネットワーク
(172.17.0.0/24)
(172.17.0.6)
42
(HCNK)
(172.17.0.7)
41a
5
(HI)
ホームイントラネット
(10.0.0.0/24)
(10.0.0.1)
(10.0.0.2)
(10.0.0.3)
(10.0.0.4)
51
(FW1)
61
(HCND)
(172.17.0.1)
ホームコントロールイントラネット
(172.17.0.0./24)
6
(HCI)
HCND4
HCND1
HCND2
HCND3
62
63
64
65
(172.17.0.5)
(172.17.0.4)
(172.17.0.3)
(172.17.0.2)

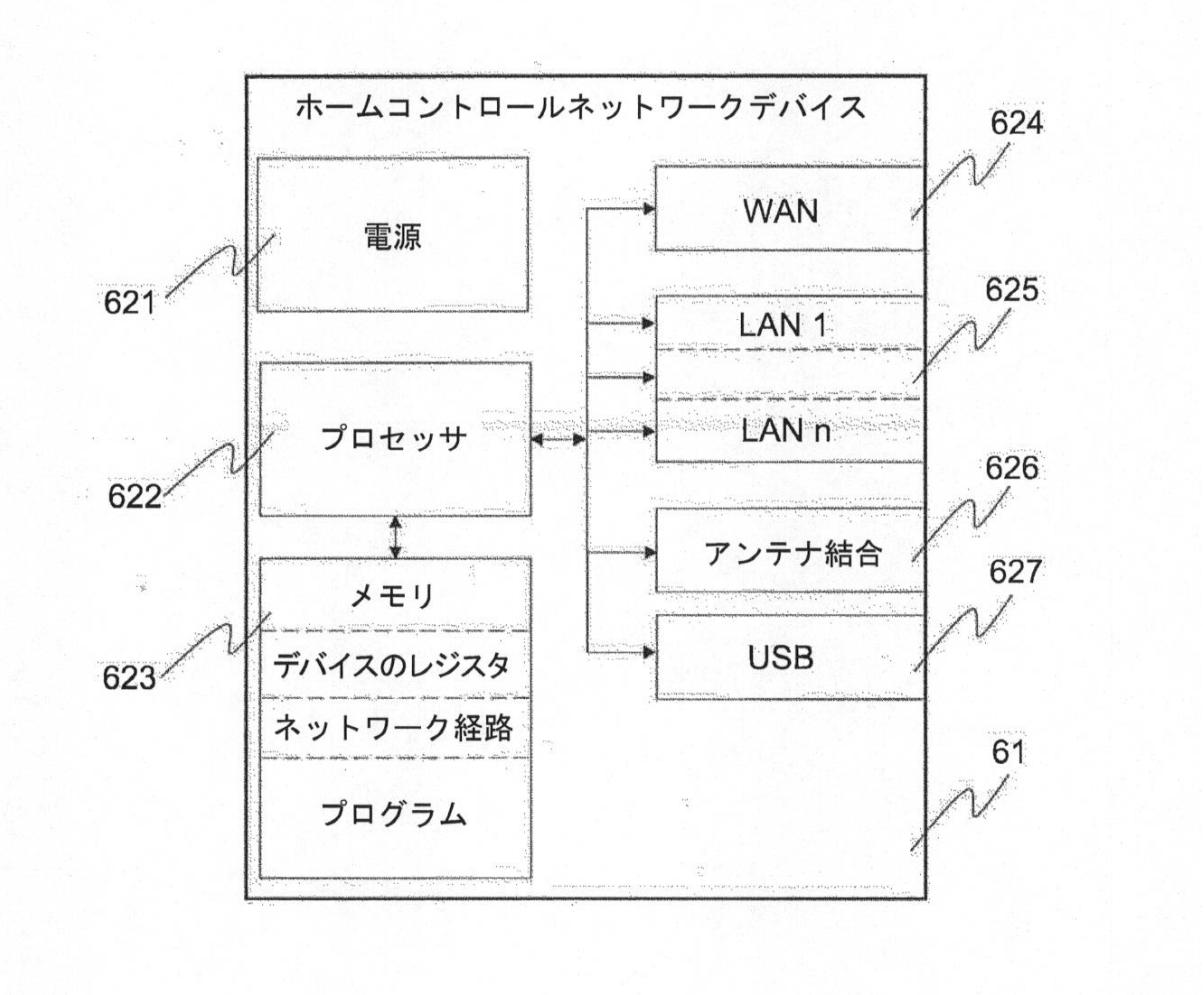
【図２】


(HCN)
1B
2
インターネット
(240.2.1.2)
(HCNS)
21
(240.1.1.1)
(240.1.1.2)
VPN
55
(HI)
5
ハウスイントラネット
(10.0.0.0/24)
(10.0.0.1)
(10.0.0.2)
(10.0.0.4)
(10.0.0.3)
51
(FW1)
(HCI)
6
ハウスコントロールイントラネット
(172.17.0.0./24)
(172.17.0.1)
(HCND)
61
62
(172.17.0.5)
63
(172.17.0.4)
HCND1
64
(172.17.0.3)
HCND2
65
(172.17.0.2)
HCND3
HCND4
3
パブリック
ネットワーク/
イントラネット
(10.0.1.0/24)
(10.0.1.2)
(10.0.1.1)
31
(FW2)
41c
(HCNK)
42e
USB
42b

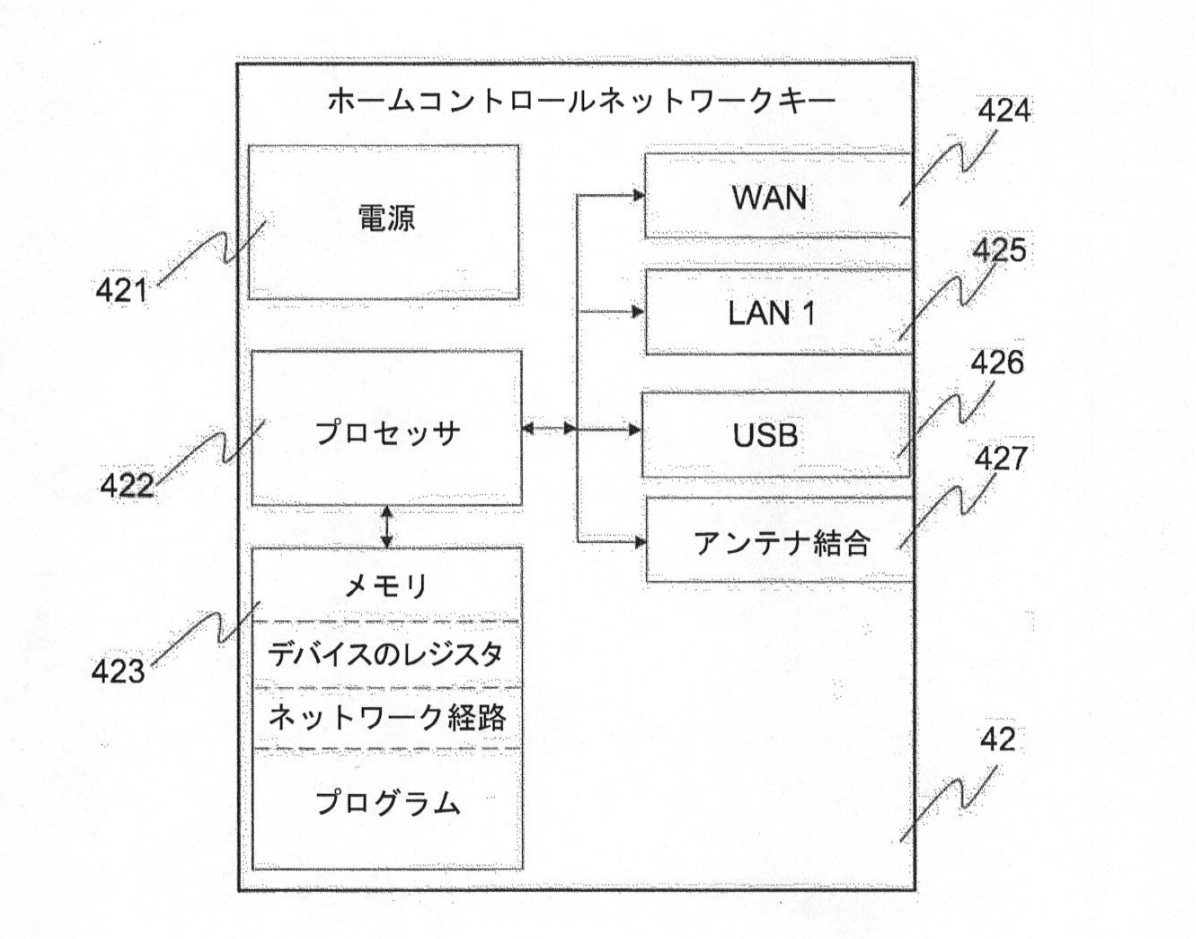
【図３】


300
ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーがネットワークに接続される
301
ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーのネットワーク経路を取得する
302
取得されたネットワーク経路をホームコントロールネットワークサーバに記憶する
303
両方のネットワーク経路が記憶された?
Ei
Kyllä
304
ホームコントロールネットワークおよびホームコントロールネットワークキーが、ホームコントロールネットワークサーバにネットワーク経路を要求する
305
ホームコントロールネットワークサーバが、ネットワーク経路情報を両方のデバイスに送信する
306
ホームコントロールネットワークデバイスおよびホームコントロールネットワークキーが、それらの間のVPNトンネルを形成する
307
クライアントデバイスおよび対象のデバイスが、VPNネットワークに接続される
308
クライアントデバイスと対象のデバイスとが互いに情報を交換する
309
接続がアクティブか?
Kyllä
Ei
310
接続を確立する新たな試み?
Ei
Kyllä
311
VPN接続を解放する
312
所定の遅延
313
ホームコントロールネットワークサーバの接続を調べる
314
ホームコントロールネットワークサーバの接続が存在する?
Ei
Kyllä

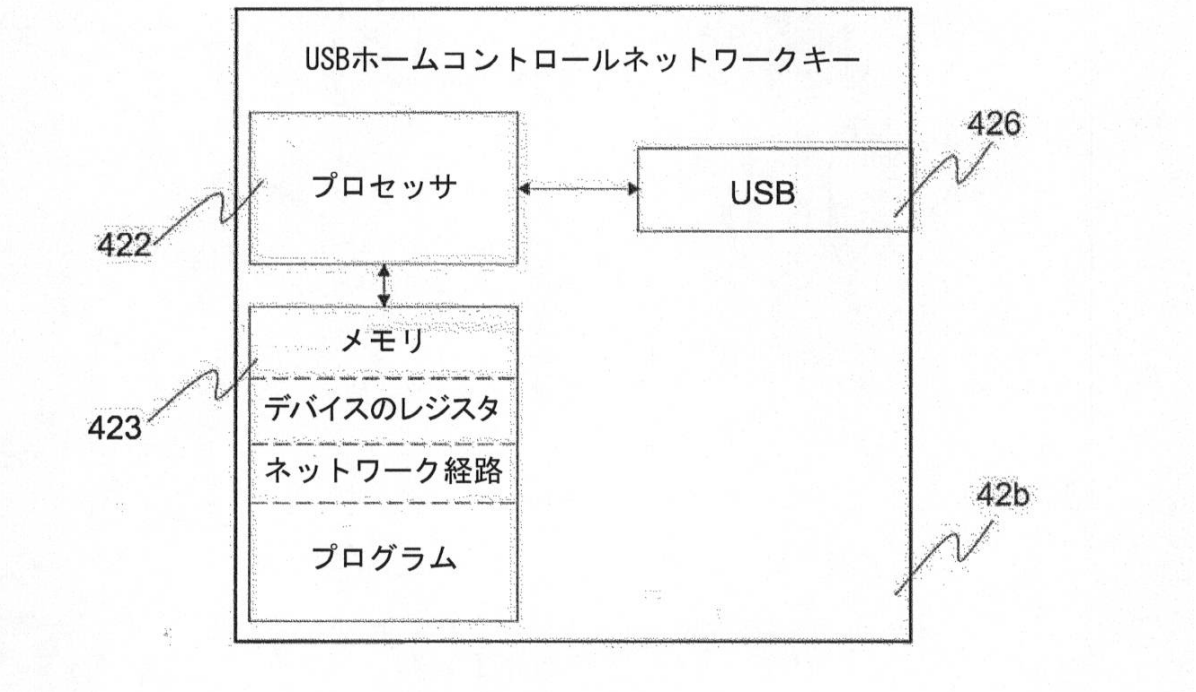
【図４】


ホームコントロールネットワークデバイス
電源
621
プロセッサ
622
メモリ
623
デバイスのレジスタ
ネットワーク経路
プログラム
WAN
624
LAN 1
625
LAN n
アンテナ結合
626
USB
627
61

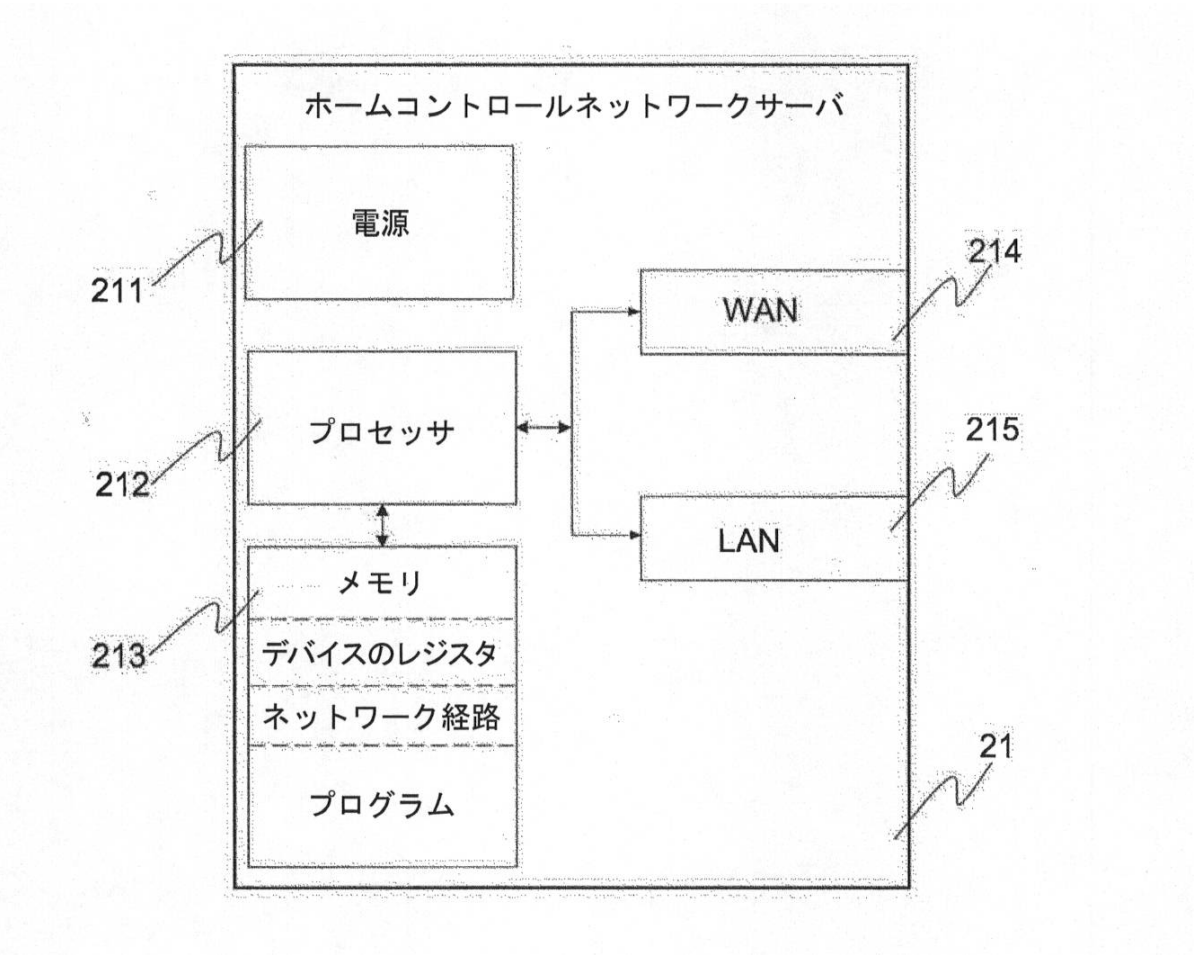
【図５ａ】


ホームコントロールネットワークキー
424
電源
WAN
421
425
LAN 1
426
プロセッサ
USB
422
427
アンテナ結合
メモリ
423
デバイスのレジスタ
ネットワーク経路
42
プログラム

【図５ｂ】


USBホームコントロールネットワークキー
426
プロセッサ
USB
422
メモリ
423
デバイスのレジスタ
ネットワーク経路
42b
プログラム

【図６】


ホームコントロールネットワークサーバ
電源
211
WAN
214
プロセッサ
212
215
LAN
メモリ
213
デバイスのレジスタ
ネットワーク経路
プログラム
21

フロントページの続き

審査官　安藤　一道

(56)参考文献　特開２００７－２３５６３８（ＪＰ，Ａ）
特開２００６－３４４０１７（ＪＰ，Ａ）
国際公開第２０１２／１１３９７５（WO，Ａ１）
欧州特許出願公開第１９１２４１３（ＥＰ，Ａ１）
米国特許出願公開第２００３／２１４９５５（ＵＳ，Ａ１）
米国特許出願公開第２０１０／１２５８９４（ＵＳ，Ａ１）
米国特許出願公開第２００９／０６６７８９（ＵＳ，Ａ１）
米国特許第７３９１２９８（ＵＳ，Ｂ１）
米国特許出願公開第２０１０／０１４５２９（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２８
Ｈ０４Ｌ　１２／７０