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

特許第6293050号
(P6293050)

(45)発行日　平成30年3月14日(2018.3.14)　(24)登録日　平成30年2月23日(2018.2.23)

(51)Int.Cl.		F I		
H04L 12/70	(2013.01)	H04L	12/70	A
G06F 13/00	(2006.01)	G06F	13/00	353C
H04L 12/24	(2006.01)	H04L	12/24	
H04L 29/08	(2006.01)	H04L	13/00	307A

請求項の数 11　(全 12 頁)

(21)出願番号　特願2014-517671 (P2014-517671)
(86)(22)出願日　平成24年6月27日(2012.6.27)
(65)公表番号　特表2014-526162 (P2014-526162A)
(43)公表日　平成26年10月2日(2014.10.2)
(86)国際出願番号　PCT/EP2012/062415
(87)国際公開番号　WO2013/000936
(87)国際公開日　平成25年1月3日(2013.1.3)
審査請求日　平成27年6月22日(2015.6.22)
審判番号　不服2017-2865 (P2017-2865/J1)
審判請求日　平成29年2月28日(2017.2.28)
(31)優先権主張番号　11447015.6
(32)優先日　平成23年6月29日(2011.6.29)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　501263810
トムソン　ライセンシング
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ
フランス国，　９２１３０　イツシー　レ　ムーリノー，　ル　ジヤンヌ　ダルク，　１－５
１－５，　ｒｕｅ　Ｊｅａｎｎｅ　ｄ’Ａｒｃ，　９２１３０　ＩＳＳＹ　ＬＥＳ　ＭＯＵＬＩＮＥＡＵＸ，　Ｆｒａｎｃｅ
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】デバイスの遠隔管理

(57)【特許請求の範囲】

【請求項１】

遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成デバイスと遠隔構成可能デバイスとの間の通信方法であって、

前記遠隔構成デバイスにより、前記遠隔構成可能デバイスとの前記遠隔管理接続が失われたと判定された場合、

前記遠隔構成デバイスにより、前記遠隔管理接続以外の接続で、前記遠隔構成可能デバイスにより前記失われた遠隔管理接続の再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを、前記遠隔構成可能デバイスのアドレス及び前記遠隔構成可能デバイスの所定のポート番号に送信するステップと、

前記遠隔構成デバイスにより、前記メッセージに含まれる前記情報の前記遠隔構成可能デバイスによる使用結果及び前記少なくとも１つのコマンドの前記遠隔構成可能デバイスによる適用結果である、前記遠隔管理接続の再確立の要求を受信するステップと

を有することを特徴とする方法。

【請求項２】

前記所定のポート番号は、前記遠隔管理接続が失われた場合に、前記遠隔構成可能デバイスが前記遠隔構成デバイスと前記遠隔管理接続を再確立することを可能にするメッセージを前記遠隔構成可能デバイスが受信するポート番号である、請求項１に記載の方法。

【請求項３】

前記情報は、前記遠隔構成デバイスのアドレスを有する、請求項１又は２に記載の方法

。
【請求項４】
前記情報は、接続要求証明書を有する、請求項１ないし３のうちいずれか１項に記載の方法。
【請求項５】
遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成可能デバイスと遠隔構成デバイスとの間の通信方法であって、
前記遠隔構成デバイスにより、前記遠隔管理接続が失われたと判定された場合、
前記遠隔構成可能デバイスにより、前記遠隔管理接続以外の接続で、失われた前記遠隔管理接続の前記遠隔構成可能デバイスによる再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを所定のポート番号で受信するステップと、
前記遠隔構成可能デバイスにより、前記少なくとも１つのコマンドを適用するステップと、
前記遠隔構成可能デバイスにより、前記遠隔構成可能デバイスによる前記メッセージに含まれる前記情報の使用結果及び前記少なくとも１つのコマンドの前記適用の結果である、前記失われた遠隔管理接続の再確立の要求を前記遠隔構成デバイスに送信するステップと
を有することを特徴とする方法。
【請求項６】
前記所定のポート番号は、前記遠隔管理接続が失われた場合に、前記遠隔構成可能デバイスが前記遠隔構成デバイスと前記遠隔管理接続を再確立することを可能にするメッセージを前記遠隔構成可能デバイスが受信するポート番号である、請求項５に記載の方法。
【請求項７】
前記情報は、前記遠隔構成デバイスのアドレスを有する、請求項５又は６に記載の方法。
【請求項８】
前記情報は、接続要求証明書を有する、請求項５ないし７のうちいずれか１項に記載の方法。
【請求項９】
遠隔管理接続を介してデジタル通信ネットワークで遠隔構成デバイスに相互接続された遠隔構成可能デバイスであって、
前記遠隔管理接続以外の接続で、失われた前記遠隔管理接続の前記遠隔構成可能デバイスによる再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを所定のポート番号で受信する接続要求サーバと、
前記メッセージに含まれる前記情報の使用結果及び前記少なくとも１つのコマンドの適用結果である、前記失われた遠隔管理接続の再確立の要求を前記遠隔構成デバイスに送信するクライアントモジュールと
を有することを特徴とする遠隔構成可能デバイス。
【請求項１０】
前記接続要求サーバ及び前記クライアントモジュールは、前記遠隔構成可能デバイスの他のモジュールと独立して機能する、請求項９に記載の遠隔構成可能デバイス。
【請求項１１】
遠隔構成可能デバイスと遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成デバイスであって、
前記遠隔構成可能デバイスとの前記遠隔管理接続が失われたと判定するように構成された中央処理装置と、
前記遠隔管理接続以外の接続で、前記遠隔構成可能デバイスにより前記失われた遠隔管理接続の再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを、前記遠隔構成可能デバイスのアドレス及び所定のポート番号に送信するように構成された接続要求クライアントと、

前記メッセージに含まれる前記情報の前記遠隔構成可能デバイスによる使用結果及び前記少なくとも１つのコマンドの前記遠隔構成可能デバイスによる適用結果である、前記遠隔管理接続の再確立の要求を受信するように構成されたサーバと
を有することを特徴とする遠隔構成デバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、デバイスの遠隔管理の分野に関し、方法を実施するデバイスに関する。特に、本発明は、遠隔管理可能デバイスと遠隔管理サーバとの間に遠隔管理通信が失われた場合に使用可能なデバイスの遠隔管理のためのライフライン接続に関する。

【背景技術】

【０００２】

家庭内でのサービス加入デバイス（例えば、いわゆるトリプルプレイゲートウェイ（VoIP電話（Voice over Internet Protocol）、インターネット、IPテレビ））の出現により、サービスオペレータにより提示されるサービスを満足に使用／受信することができるように正確にサービス加入デバイスを構成するために、これらのサービス加入デバイスを管理する方法についてサービスオペレータにとって問題が生じている。特に、サービスオペレータは、新たなサービスを提供するために又は既存のサービスを改善するために、オペレータにより提供されるホームゲートウェイにおいて、追加ソフトウェアのインストール、ファームウェアのアップグレード、既存のソフト又はハードウェアの構成を頻繁に行う必要がある可能性がある。

【０００３】

対策は、例えばCPE又はサービス加入デバイスの遠隔構成のためのTR-069仕様に従って、これらのサービス加入デバイスを専用の構成デバイス又は自動構成サーバ（ACS：Auto Configuration Server）に接続することを含む。ACSは、必要なソフトウェアをサービス加入デバイスに自動的に配信する役目をする。TR-069は、ゲートウェイ及びルータ、オーディオビジュアル受信用のセットトップボックス、VoIP（voice over IP）電話セット、並びにNAS（Network Attached Storage）のようなデバイスによりサポートされている。

【０００４】

しかし、ACSとCPEデバイスとの間の通信が明らかに失われた場合（切断された場合）、既存の対策は失敗する。例えば、TR-069の場合、CPEデバイスは、自動構成サーバ（ACS）との管理セッションを確立する役目をする。ACSは、いわゆる“接続要求（connection request）”により、いつでもCPEに対して管理セッションを確立することを起動させることができる。認証のような更なるセキュリティ手段を有する遠隔管理を可能にするためのこの比較的複雑な手段は、遠隔管理のセキュリティを確保する。TR-069は、ロバストなプロトコルであるように設計されているが、ACSがCPEに対してACSとの遠隔管理接続を確立することを起動させることに成功しない状況が存在する。この失敗の理由は、TLS（Transport Layer Security）証明書の失効を含む。これは、CPEがACSをもやは信頼しないことを生じるため、ACSとの管理接続を確立することを拒否する。CPEにおける構成の問題は、例えば、CPEがACSのURL（Uniform Resource Locator）を失ったこと、CPEが不適切なACS認証証明書を有すること、CPEが長期間に電源オフ状態になっているためCPEデバイスに通信されなかったネットワークトポロジの変化、又は、CPEデバイスに対する制御を得る理由で遠隔管理を無効にするための、例えばハッキングによる自発的なエンドユーザの介入がある。遠隔管理接続のこの欠落は、サービスプロバイダにとって大きな問題をもたらす。この理由は、遠隔管理接続が監視、診断、構成管理又はファームウェアのアップデートに使用されるからである。もはや管理可能ではないデバイスは、QoS（Quality of Service）、セキュリティ又はファイヤウォールサービス、IPTV（Internet Protocol Television）のようなサービス、VoIPの追加及び電話番号の構成のような新たなサービス、劣化した接続、劣化したサービス品質のようないずれか報告された問題の診断又はトラ

ブル対応、及びバグを解決するため又は新たなデバイス機能を導入するための自動ファームウェアアップグレードを使用するために必要な構成の更新をもはや受信することができない。CPEがACSの正確な位置（アドレス）を失った場合、又は有効な認証情報を失った場合、CPEは、ACSにとって“失われた（lost）”と考えられる。この理由は、CPEがサーバへの管理接続をうまく確立することができないからである。このような場合、サービスオペレータと加入デバイスとの間の通信は、明らかに失われており、オペレータの手動介入のみにより（ユーザへの命令又はユーザの敷地へのエンジニアの派遣により）復旧可能である。

【０００５】

2003年12月23日の文献WO03/107133 A2“Secure Remote Management Appliance”（SMRA）は、ネットワークサービスへの既存の接続を失うことと、他のインタフェースでネットワークサービスへの接続を再確立することとを記載している。他の更なるネットワークインタフェースでネットワーク管理局に連絡を試みるが、前述の問題（前述「この失敗の理由」を参照のこと）の１つが生じている場合、依然としてSMRAがネットワーク管理局に連絡できない。この理由は、ネットワークインタフェースの変更は、これらの失敗の理由を除去しないからである。

【０００６】

2009年9月10日の文献US2011/060822 A1“Apparatus and method for managing communications”は、周辺のゲートウェイに対して自身のために管理接続を設定するように要求することにより、WAN接続のロスを管理するゲートウェイについて記載している。これは、前述の問題が生じた場合にゲートウェイがWLAN接続を復旧することを可能にしない。この理由は、例えば適切な証明書を提供することができない場合、失敗したゲートウェイは代替の管理接続を設定することができないからである。更に、この対策は、失敗したゲートウェイが周辺のゲートウェイと通信することができることを要求する。これは、ネットワークトポロジが変化したときに不可能になる可能性がある。

【発明の概要】

【発明が解決しようとする課題】

【０００７】

従って、サービスプロバイダの観点から失われたと考えられるデバイスの遠隔管理接続の再確立をサポートし、デバイスの高コストな物理的な再配置又は顧客の介入の必要性を回避するために、顧客の家庭に配置されたオペレータのサービス加入デバイスの遠隔構成管理の最適化の必要性が存在する。

【０００８】

本発明は、従来技術の不都合な点のうち少なくともいくつかを軽減することを目的とする。

【０００９】

より具体的には、本発明は、サービスオペレータのサービス加入デバイス又はCPEの最適化された遠隔管理を可能にする。

【課題を解決するための手段】

【００１０】

この趣旨で、本発明は、遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成デバイスと遠隔構成可能デバイスとの間の通信方法を提案する。この方法は、遠隔構成デバイスにおいて、遠隔管理接続が失われたと判定された場合、遠隔管理接続以外の接続（2001）で、遠隔構成可能デバイスにより失われた遠隔管理接続の再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを、遠隔構成可能デバイスのアドレス及び遠隔構成可能デバイスの所定のポート番号に送信するステップと、メッセージに含まれる情報の遠隔構成可能デバイスによる使用結果及び少なくとも１つのコマンドの遠隔管理デバイスによる適用結果である、遠隔管理接続の再確立の要求を受信するステップとを有する。

【００１１】

本発明はまた、遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成可能デバイスと遠隔構成デバイスとの間の通信方法を提案する。この方法は、遠隔構成可能デバイスにおいて、遠隔管理接続が失われたと判定された場合、遠隔管理接続以外の接続で、失われた遠隔管理接続の遠隔構成可能デバイスによる再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを所定のポート番号で受信するステップと、少なくとも１つのコマンドを適用するステップと、メッセージに含まれる情報の使用結果及び少なくとも１つのコマンドの適用結果である、失われた遠隔管理接続の再確立の要求を遠隔構成デバイスに送信するステップとを有する。

【００１２】

変形実施例によれば、所定のポート番号は、遠隔管理接続が失われた場合に、遠隔構成可能デバイスが遠隔構成デバイスと遠隔管理接続を再確立することを可能にするメッセージを遠隔構成可能デバイスが受信するポート番号である。

【００１３】

変形実施例によれば、情報は、失われた遠隔管理接続を再確立するために使用される接続要求証明書を有する。

【００１４】

変形実施例によれば、情報は、失われた遠隔管理接続が再確立される遠隔構成デバイスのアドレスを有する。

【００１５】

本発明はまた、遠隔管理接続以外の接続で、失われた遠隔管理接続のデバイスによる再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージをデバイスの所定のポート番号で受信する接続要求サーバと、メッセージに含まれる情報のデバイスによる使用結果及び少なくとも１つのコマンドのデバイスによる適用結果である、失われた遠隔管理接続の再確立の要求を遠隔構成デバイスに送信するクライアントモジュールとを有するデバイスを有する。

【００１６】

デバイスの変形実施例によれば、接続要求サーバ及びクライアントモジュールは、デバイスの他のモジュールと独立して機能する。

【図面の簡単な説明】

【００１７】

【図１】本発明が実装される例示的なネットワークインフラストラクチャ

【図２】本発明を実装する図１のデバイス104及び106/108/110/111に追加される追加モジュール201及び204

【発明を実施するための形態】

【００１８】

本発明の更なる利点は、本発明の特定の非限定的な実施例の説明を通じて明らかになる。実施例について、図面を参照して説明する。

【００１９】

図１は、本発明が実装される例示的なネットワークインフラストラクチャを示している。

【００２０】

ネットワークインフラストラクチャは、

・一式のプロバイダサーバ100-103（例えば、ウェブサーバ100、ビデオオンデマンド（VoD：Video On Demand）サーバ101、ブロードバンド放送サーバ102及びVoIPサーバ103）
・構成サーバ（CS：configuration server）104
・ゲートウェイ（GW：gateway）デバイス106（CPE）
・アクセスネットワーク105（例えば、インターネット又は専用ネットワークであり、アクセスネットワークは、（接続1000を介して）プロバイダサーバ100-103と、（接続1001を介して）サーバ104と、（接続1002を介して）ゲートウェイ106とを相互接続する）
・ローカルネットワーク107（ホームネットワークのデバイスを相互接続し、これらを（

接続1004、1005及び1006を介して）ゲートウェイ106を介してアクセスネットワーク105に接続し、アクセスネットワーク105に接続された他のデバイス（100-103、104）に接続する）
・パーソナルコンピュータ（PC：personal　computer）108（CPE）
・テレビセット109
・セットトップボックス（STB：set　top　box）110（CPE）
・無線PC111（CPE）
を有する。

【００２１】

ゲートウェイ106は、トリプルプレイサービスを加入者に提供するオペレータにより提供されるデバイスである。ゲートウェイ106は、加入者に対して、
・IPTVセットトップボックス110及びTVセット109を介した論理接続2002でオペレータのブロードバンド放送サーバ（それぞれ101及び102）により提供されるVoDテレビ及びIP放送サービスにアクセスすること
・論理接続2003を介してウェブサーバ100により提供されるサービスである、PC108及び111を介してインターネットにアクセスすること
・論理接続2003を介してVoIPサーバ103により提供されるサービスである無線DECT（Digital　Enhanced　Cordless　Telecommunications）電話セット（図示しないデバイス）でのIP電話サービスにアクセスすること
を可能にする。

【００２２】

実線1000、1001及び1001は、物理接続である。破線2001-2003は論理接続である。破線2001は、本発明による論理ライフライン接続を示す。破線2002は、構成サーバ104とゲートウェイCPEデバイス106との間の論理遠隔管理接続を示す。破線2003は、１つ以上のサービスプロバイダサーバ100-103とゲートウェイ106との間の論理接続を示す。破線はゲートウェイ106を中心点に有するように図示されているが、これらの破線は、CPEデバイス108、110及び111と、プロバイダサービスサーバ100-103及び構成サーバ104とのいずれも接続できる点に留意すべきである。

【００２３】

プロバイダが構成又はソフトウェアの更新を１つ以上のCPE（106、108、110、111）に送信しようとする場合、遠隔管理接続2002を使用して手動の介入なしに（すなわち、オペレータの技術サービスが加入者の敷地に介入する必要なく）、選択されたCPEデバイスを自動的に更新又は再構成する構成サーバ104に対して命令する。特に、構成サーバ104は、遠隔管理接続2002を使用して、ゲートウェイ106に格納された構成サーバのアドレスを変更することができる（例えば、加入者の数の増加のため更なる構成サーバが必要な場合、又はIPアドレスの再配布の場合（すなわち、構成サーバのアドレスに影響を及ぼすネットワークトポロジの変更の場合））。しかし、１つ以上の加入者のCPEデバイスがネットワーク105又は107から切断されている場合、或いは、電源が落とされている場合、アドレスの更新はこれらのデバイスに伝わることはできない。その後、これらのいくつかは、構成サーバによる構成管理にとって到達不可能になる可能性がある（すなわち、遠隔管理接続2002は失われたと考えられる）。このことは、関与するCPEデバイスの誤った動作を生じる可能性がある。他のシナリオによれば、遠隔管理接続2002での構成管理セッション中にCPEに配信されるソフトウェアの更新は、リブート時にCPEのオペレーティングシステムのクラッシュを生じる可能性がある。この場合、関与するCPEは、明らかに故障中になり、もはや構成管理のために構成サーバにより到達できなくなり、加入者はもはや加入しているサービス（例えば、電話サービスを含む）にアクセスすることができなくなる。更に他のシナリオでは、加入者のホームネットワークの１つ以上のCPEデバイスは、構成サーバにより送信された誤った構成のため、構成サーバにより管理不能になる（CPEデバイスは管理接続を確立しなければならない点に留意すべきである。管理接続を設定するために必要なデータが誤っている場合、遠隔管理接続2002はCPEデバイスにより設定できない）。

更に他のシナリオでは、TLS（Transport Layer Security）セキュリティ証明書が失効し、CPEデバイスがもはや構成サーバを信頼しなくなり、従って、CPEデバイスが管理セッションを再確立することを拒否する。全てのこれらのシナリオ及び説明しない他のシナリオは、遠隔構成接続2002のロスを生じるため、CPEデバイスを構成管理にとって到達不可能にする。

【００２４】

従って、本発明は、CPEデバイスがACSにとって管理不能になった場合、すなわち、遠隔管理接続2002が失われた場合、CPEデバイスの正確な機能を復旧させることを可能にするライフライン接続2001を追加する。図２において、ライフライン接続2001は、構成サーバ104をゲートウェイ106に接続する。変形実施例によれば、ライフライン接続2001は、CS104以外の他のデバイス（図示せず）に接続される。これは、例えば、アドホックデバイスからゲートウェイ106を‘トラブル対応’することを可能にする。

【００２５】

図２は、本発明を実装するデバイス104及び106に追加される追加モジュール201、204及び207を示している。これらのモジュールは、点線のボックス209で図２に示されている。構成サーバ（“CS”又は“ACS”）側において、接続要求クライアント201が構成サーバ104に追加される。CPE側（106、108、110又は111）において、接続要求サーバ203及び固定記憶空間207が追加される。CS104の接続要求クライアント201は、接続2001でCPEの接続要求サーバと通信する。サービスプロバイダは、接続2003を介してCPEデバイスのいずれかにそのサービスを提供する。

【００２６】

構成管理セッション中に、CPEデバイス（106、108、110又は111）のHTTPクライアント205は、遠隔管理接続2002を介してCS104のHTTPサーバ202と通信する。特定の実施例によれば、HTTPサーバ202及びHTTPクライアント204は、TR-069プロトコルに従ってこの接続2002で通信する。モジュール200及び208は、それぞれ構成サーバ104及びゲートウェイ106の通常の機能に必要なモジュールである。これらのモジュールは、例えば、CPU（Central Processing Unit）、メモリ、ファイヤウォール、NAT（Network Address Translation）モジュール等を有する。モジュールは、構成サーバ104の内部バス203及びデバイス106、108、110又は111の内部バス206のような内部通信手段を介して相互に通信する。

【００２７】

接続2001は、図１について前述した網羅的でない通信失敗シナリオにより遠隔管理通信リンク2003が失われたときに、遠隔管理通信リンク2003を復旧させることを可能にするデバイス106、108、110及び111へのライフライン接続を構成する。

【００２８】

デバイス106、108、110又は111の接続要求サーバ（CRS：Connection Request Server）204の役目は、サーバとして機能し、所定のポート番号（例えばTCPポート7547）で入来する接続要求（すなわち、HTTP GETリクエスト）を受信することである。このポートは、以下ではライフライン接続ポートと呼ばれる。CRSは、一式のCPE構成の証明書（例えば、工場出荷時のユーザ名及びパスワード）を用いて要求を発行したエンティティを更に認証する。本発明の変形実施例によれば、CPEは、悪意のある使用に対して保護することを可能にするもののような任意選択の機構を備える。例示的な保護機構は、サービス妨害攻撃に対してCPEを保護するために、時間によって許可される要求の数を制限することを可能にする接続要求の調整（throttling）である。CPEは、多くの要求に同時にサービス提供しているときに、利用不可能になる。

【００２９】

デバイス106、108、110又は111のHTTPクライアント205の役目は、場合によって構成サーバ104のIPアドレスを取得するために１つ以上のDNSサーバ（図示せず）へのDNS（Domain Name System）クエリを介して構成サーバのURL（Unified Resource Locator）を解決した後に、構成サーバ104との遠隔構成接続2002で通信するHTTPクライアントとして機能する。CS104への接続は、複数のイベントの発生時に確立される。例えば、接続要求がC

RS204によりライフライン接続2001で受信された場合、CRSは、このようなイベントをHTTPクライアントに通知する。また、デバイス106、108、110又は111のスタートアップ時、或いはデバイス106、108、110又は111のデバイス構成が変更し、加入しているCS104がこのような変更を通知される場合に確立される。変形実施例によれば、CS140への接続の確立を起動させるイベントのリストは、TR-069 Inform RPC（Remote Procedure Call）イベントを有する。デバイス106、108、110又は111のHTTPクライアント205は、CS104を信頼するために、複数のローカルに格納された証明書（例えば、固定記憶装置107にローカルに格納される）のいずれかを用いて、CS104により提供された証明書の署名を更に確認し、HTTPクライアント205は、CS104から受信したコマンドを適用する。このコマンドは、例えば、固定記憶装置207に格納されたデバイス106、108、110又は111の特定の構成パラメータを変更するための‘SetParameterValues’又は‘Reboot’を有する。

【００３０】

デバイス106、108、110又は111の固定記憶装置207の役目は、

・CS URL（例えば、http://cs.provider.com）を有すること

・接続要求証明書（ユーザ名及びパスワード）を有すること

・CSプロバイダの証明書の署名を確認するために再利用可能な１つ以上のローカルに格納された証明書を有すること

・ファームウェアイメージ及び他の製造者により提供されたデータの信憑性を確認するために使用されるデバイス106、108、110又は111の製造者の公開鍵を有すること

・デバイス106、108、110又は111のCPEデバイス構成を有すること

である。

【００３１】

CS104の接続要求クライアント（CRC）201は、例えば、特定の時点に接続要求を開始し、デバイス106、108、110又は111に対して認証し、遠隔構成可能デバイスのよる管理セッションの確立を起動するHTTPクライアントである。

【００３２】

CS104のHTTPサーバ202の役目は、特に、HTTPサーバを提供し、CSの証明書の署名をデバイス106、108、110又は111に提供することである。

【００３３】

図２において、デバイス106、108、110又は111は、例示的なCPEデバイスとして挙げられている。しかし、本発明は、これらの種類のデバイスでの実装に限定されず、如何なる種類のCPEに実装されてもよい。

【００３４】

遠隔構成接続2002が失われた場合、CS104のCRS204は、ライフライン接続ポートで受信するように構成される。特定の実施例によれば、このような機構はウォッチドッグ（watchdog）機構により実装される。この場合、本発明を実装するデバイスの他のモジュールのうち１つは、キープアライブ（keep alive）信号をCRS204に定期的に送信する。キープアライブ信号がウォッチドッグタイマの満了後に受信されない場合、CRSのリスト処理が自動的に開始される。他の実施例によれば、受信処理は常にアクティブである。最初の実施例は、例えば、受信処理（及び受信処理を実装するために必要なモジュール）が常に電源投入されたままになっている必要はないため、本発明を実装するデバイスの電力消費を低減することを可能にする。

【００３５】

CPEのIPアドレスは、典型的にはサービスオペレータにより知られている。ライフライン接続ポート番号は、例えばTR-069についてIANA（Internet Assigned Numbers Authority）により固定された初期設定のポート番号（TCPポート7457）である。或いは、サービスプロバイダとCPEデバイス製造者との間で合意される。CPE（例えば、GW106）がライフライン接続ポートで入来するHTTP GET接続要求メッセージ（すなわち、救済メッセージ）を受信した場合、CPEのCRS（例えば、GW106のCRS204）は、救済メッセージを確認する。CPEが遠隔構成デバイスとの失われた遠隔管理接続を再確立することを可能にするた

めに、救済メッセージは、救済情報と救済コマンドとを有する。典型的な救済情報は、デバイスエンティティ（例えば、製造者ID、製品クラス、シリアル番号を有し、これは、救済コマンドが目的のCPEデバイスのみにより考慮されることを確保する）、有効なACS URL等である。典型的な救済コマンドは、
・工場出荷時に戻ること（場合によってはCSとの遠隔管理接続を失ったことをもたらしたユーザ構成又は他の構成の変更を取り消すため）
・救済情報で提供される新たなCS URLを使用すること
・CSの証明書（ユーザ名、パスワード）を救済情報で提供された証明書に設定すること
・とにかくCSを信頼するためにCSの証明書の検査を無効にすること、又は
・サービスプロバイダがデバイスに接続して管理することを可能にするため（例えば、構成の問題をトラブル対応して訂正するため）、ユーザインタフェース、Telnetセッションのような他の管理インタフェースを開くこと
を有する。任意選択で、ライフライン接続2001での救済メッセージのコマンドのセキュリティを向上させて悪意のある送信に対して保護するため、救済メッセージの情報は、CPE製造者の秘密鍵で署名された救済メッセージのコマンドで計算されたハッシュ値を有する。これにより、CPEデバイスは、救済コマンドが不正なエンティティにより変更されていないいことを検査することができる。

【００３６】

救済メッセージがCPEにより正確に認証された場合、CPEは救済コマンド（例えば、新たなファームウェアのダウンロード）を実行する。救済コマンドの適用後、CPEは適切に再構成され、CPEは遠隔管理接続の再確立の要求をCSに送信する。この要求は、場合によっては救済メッセージで提供される情報（すなわち、提供される新たなACS URLの使用、或いは換言すると、遠隔構成デバイスのアドレス）に基づき、場合によっては、救済メッセージで提供された情報で提供された少なくともいくつかの情報（すなわち、認証に有効な提供された新たな接続要求証明書）を有する。従って、要求は、救済メッセージで提供された情報の遠隔構成可能デバイスによる使用結果及び救済メッセージに含まれる救済コマンドの遠隔管理デバイスによる適用結果である。

【００３７】

変形実施例によれば、CPEデバイスは、コマンドが考慮されたことを示す確認メッセージをライフライン接続2001でCSに送信することにより、救済コマンドが考慮されたことを確認する。この変形は、CPEが遠隔管理セッションを確立する用意ができている場合、その正確な時間を構成サーバに伝達するという利点を有する。

【００３８】

変形実施例によれば、救済メッセージは、CPEにより実行される複数の救済コマンドを有する。

【００３９】

変形実施例によれば、CSは、複数の救済コマンドを適用するために、ライフライン接続2001で複数の救済メッセージを送信する。任意選択で、それぞれ後続の救済メッセージは、前に送信された救済メッセージがCPEにより考慮されたことを確認する前述の確認メッセージを受信した後にのみ送信される。

【００４０】

更に他の変形実施例によれば、CPEは、救済メッセージを考慮した後に、CSに連絡できるか否かを確認し、これをライフライン接続2001で返信する。

【００４１】

変形実施例によれば、本発明を実装するために必要な構成要素（接続要求サーバ204及びクライアントモジュール205）は、自動的に機能する。すなわち、遠隔構成可能デバイスの他のモジュールと独立して機能する。この場合、本発明を実装するデバイスが“クラッシュ”しても、すなわち、応答がない場合であっても、デバイスは、ライフライン接続2001を介して動作状態に戻されることが可能になる。これは、例えば、動作不能又は管理不能な状態にあるデバイスに適切な構成又は訂正されたファームウェアのバージョンをダ

ウンロードすることを可能にする。

【００４２】

変形実施例は、特定の有利な実施例を形成するように組み合わされてもよい。

【００４３】

特定の実施例によれば、本発明は、完全にハードウェアで、例えば、専用コンポーネント（例えば、ASIC（Application Specific Integrated Circuit）、FPGA（Field Programmable Gate Array）又はVLSI（Very Large Scale Integration））として実装される。或いは、デバイスに統合された別個の電子コンポーネントとして又はハードウェアとソフトウェアの組み合わせの形式で実装される。

以上の実施例に関し、更に、以下の項目を開示する。

（付記１）遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成デバイスと遠隔構成可能デバイスとの間の通信方法であって、

前記遠隔構成デバイスにおいて、

前記遠隔管理接続が失われたと判定された場合、

前記遠隔管理接続以外の接続で、前記遠隔構成可能デバイスにより前記失われた遠隔管理接続の再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを、前記遠隔構成可能デバイスのアドレス及び前記遠隔構成可能デバイスの所定のポート番号に送信するステップと、

前記メッセージに含まれる前記情報の前記遠隔構成可能デバイスによる使用結果及び前記少なくとも１つのコマンドの遠隔管理デバイスによる適用結果である、前記遠隔管理接続の再確立の要求を受信するステップと

を有することを特徴とする方法。

（付記２）前記所定のポート番号は、前記遠隔管理接続が失われた場合に、前記遠隔構成可能デバイスが前記遠隔構成デバイスと前記遠隔管理接続を再確立することを可能にするメッセージを前記遠隔構成可能デバイスが受信するポート番号である、付記１に記載の方法。

（付記３）前記情報は、前記遠隔構成デバイスのアドレスを有する、付記１又は２に記載の方法。

（付記４）前記情報は、接続要求証明書を有する、付記１ないし３のうちいずれか１項に記載の方法。

（付記５）遠隔管理接続を介してデジタル通信ネットワークで相互接続された遠隔構成可能デバイスと遠隔構成デバイスとの間の通信方法であって、

前記遠隔構成可能デバイスにおいて、

前記遠隔管理接続が失われたと判定された場合、

前記遠隔管理接続以外の接続で、失われた前記遠隔管理接続の前記遠隔構成可能デバイスによる再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを所定のポート番号で受信するステップと、

前記少なくとも１つのコマンドを適用するステップと、

前記メッセージに含まれる前記情報の使用結果及び前記少なくとも１つのコマンドの適用結果である、前記失われた遠隔管理接続の再確立の要求を前記遠隔構成デバイスに送信するステップと

を有することを特徴とする方法。

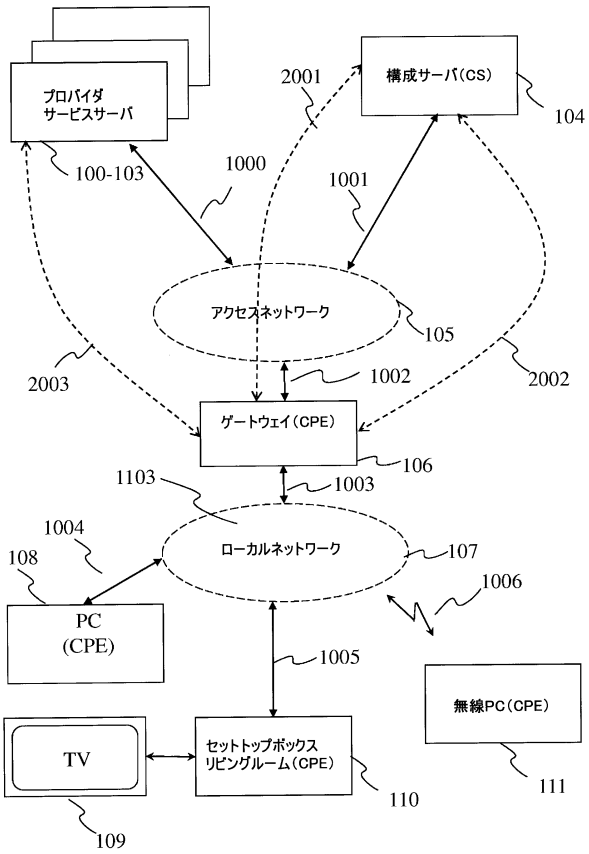
（付記６）前記所定のポート番号は、前記遠隔管理接続が失われた場合に、前記遠隔構成可能デバイスが前記遠隔構成デバイスと前記遠隔管理接続を再確立することを可能にするメッセージを前記遠隔構成可能デバイスが受信するポート番号である、付記５に記載の方法。

（付記７）前記情報は、前記遠隔構成デバイスのアドレスを有する、付記５又は６に記載の方法。

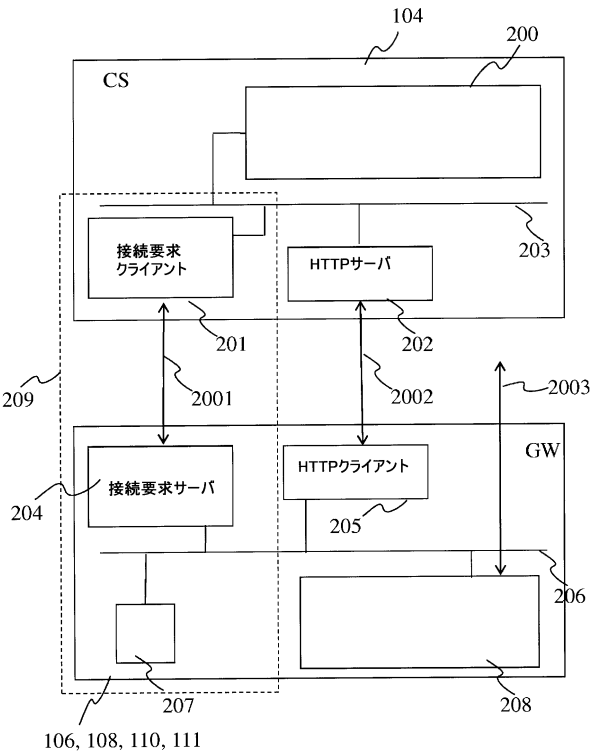
（付記８）前記情報は、接続要求証明書を有する、付記５ないし７のうちいずれか１項に記載の方法。

（付記９）遠隔管理接続以外の接続で、失われた遠隔管理接続のデバイスによる再確立を可能にする少なくとも１つのコマンド及び情報を有するメッセージを前記デバイスの所定のポート番号で受信する接続要求サーバと、
前記メッセージに含まれる前記情報の前記デバイスによる使用結果及び前記少なくとも１つのコマンドの前記デバイスによる適用結果である、前記失われた遠隔管理接続の再確立の要求を遠隔構成デバイスに送信するクライアントモジュールと
を有することを特徴とするデバイス。
（付記１０）前記接続要求サーバ及び前記クライアントモジュールは、前記デバイスの他のモジュールと独立して機能する、付記９に記載のデバイス。

【図１】



【図２】



フロントページの続き

(72)発明者　ファン・デ・ポール，ディルク
ベルギー王国，２６５０　エデゲム，プリンス・バウデウェイラーン　４７，テクニカラー　デリバリー　テクノロジーズ　ベルギー内

合議体
審判長　大塚　良平
審判官　中野　浩昌
審判官　金田　孝之

(56)参考文献　特開２００５－６５２８０（ＪＰ，Ａ）
特開２００６－８６８９７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L
G06F