

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第6067732号
(P6067732)

(45) 発行日 平成29年1月25日(2017.1.25)

(24) 登録日 平成29年1月6日(2017.1.6)

(51) Int.Cl.

G06F 13/00 (2006.01)

F 1

G 06 F 13/00 520 C

請求項の数 14 (全 19 頁)

(21) 出願番号 特願2014-541657 (P2014-541657)
 (86) (22) 出願日 平成24年11月15日 (2012.11.15)
 (65) 公表番号 特表2015-500520 (P2015-500520A)
 (43) 公表日 平成27年1月5日 (2015.1.5)
 (86) 國際出願番号 PCT/EP2012/072694
 (87) 國際公開番号 WO2013/072404
 (87) 國際公開日 平成25年5月23日 (2013.5.23)
 審査請求日 平成27年11月16日 (2015.11.16)
 (31) 優先権主張番号 11447027.1
 (32) 優先日 平成23年11月18日 (2011.11.18)
 (33) 優先権主張国 歐州特許庁 (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 イッシー レ
 ムーリノー, ル ジヤンヌ ダルク,
 1-5
 1-5, rue Jeanne d' A
 r c, 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】エンドユーザデバイス、およびそれぞれのエンドユーザデバイスの遠隔管理のためのパブリッシュ／サブスクライブプローカを備えるシステム

(57) 【特許請求の範囲】

【請求項 1】

システムであって、

ブロードバンド接続経由でサービスプロバイダネットワークに結合された複数のエンドユーザデバイスと、

前記複数のエンドユーザデバイスと通信を行うように適合されたパブリッシュ／サブスクライブプローカと、

前記サービスプロバイダネットワークに結合された第1のバックエンドエンティティであって、前記パブリッシュ／サブスクライブプローカに接続するための、および前記エンドユーザデバイスのデバイス管理を行うために制御データチャネル経由で制御データをパブリッシュするための第1のクライアントソフトウェアアプリケーションを含む、前記第1のバックエンドエンティティと、

を備え、

前記複数のエンドユーザデバイスは各々、前記制御データチャネルをサブスクライブし前記制御データを受信するために前記パブリッシュ／サブスクライブプローカに接続し、および前記制御データによる指示に応じてデバイスデータチャネル上でデバイスデータとアクションデータチャネル上でアクションデータとをパブリッシュするための第2のクライアントソフトウェアアプリケーションを含み、

当該システムは、

前記パブリッシュ／サブスクライブプローカに接続するための第3のクライアントソフ

10

20

トウェアアプリケーションを含む第2のバックエンドエンティティであって、前記複数のエンドユーザデバイスの前記デバイスデータおよび前記アクションデータをサブスクライプする、前記第2のバックエンドエンティティをさらに備える、前記システム。

【請求項2】

前記第2のクライアントソフトウェアアプリケーションは、それぞれのエンドユーザデバイスのスタートアップ時に各エンドユーザデバイス上で開始され、および事前構成されたユニフォームリソースロケータを使用することによって前記エンドユーザデバイスの前記パブリッシュ／サブスクライブプローカへの接続を確立する、請求項1に記載のシステム。

【請求項3】

前記サービスプロバイダネットワークは、インターネットサービスを提供するためのネットワークサービスプロバイダネットワークであって、前記エンドユーザデバイスの前記デバイス管理を提供する、前記ネットワークサービスプロバイダネットワークである、請求項1または2に記載のシステム。

【請求項4】

前記パブリッシュ／サブスクライブプローカは、前記ネットワークサービスプロバイダネットワークを運用するネットワークサービスプロバイダによって提供される、請求項3に記載のシステム。

【請求項5】

前記パブリッシュ／サブスクライブプローカは、インターネットサービスプロバイダによって提供される、請求項1、2または3に記載のシステム。

【請求項6】

各エンドユーザデバイスは、そのデバイス管理を行うための実行コマンドを受信するための少なくとも1つの制御データチャネルをサブスクライブする、請求項1から5のいずれか1項に記載のシステム。

【請求項7】

前記第2のバックエンドエンティティは、前記複数のエンドユーザデバイスのインベントリを保持するために前記エンドユーザデバイスのデバイスデータ、制御データおよびアクションデータをサブスクライブするが、前記エンドユーザデバイスの制御データはパブリッシュしない、請求項1から6のいずれか1項に記載のシステム。

【請求項8】

前記第2のバックエンドエンティティは、前記エンドユーザデバイスのメーカーまたはベンダーによって提供されるサーバである、請求項7に記載のシステム。

【請求項9】

前記第1のバックエンドエンティティは、前記ネットワークサービスプロバイダによって提供されるサーバである、請求項4に記載のシステム。

【請求項10】

前記エンドユーザデバイスの管理は、新しいファームウェアもしくはミドルウェアバージョンへのアップグレード、ソフトウェアアプリケーションのインストール、アップデートもしくはアンインストール、プログラムもしくはスクリプトファイルの実行、前記エンドユーザデバイスのコンフィギュレーションもしくはステータスデータに対する構造化クエリの実行、または前記エンドユーザデバイスのリセットもしくはリブートを含む、請求項1から9のいずれか1項に記載のシステム。

【請求項11】

前記エンドユーザデバイスは、制御データの署名によりバックエンドエンティティの承認の有効性を確認する、請求項の1から10のいずれか1項に記載のシステム。

【請求項12】

前記複数のエンドユーザデバイスは、同じネットワークサービスプロバイダにより配置され、

前記第1のバックエンドエンティティは、前記複数のエンドユーザデバイスの各々の前

10

20

30

40

50

記アクションデータチャネルをサブスクライブする、請求項 1 から 11 のいずれか 1 項に記載のシステム。

【請求項 1 3】

請求項 1 から 12 のいずれか 1 項に記載のシステムとオペレーションを行うように適合された、エンドユーザデバイス。

【請求項 1 4】

前記エンドユーザデバイスは、住居用ゲートウェイ、セットトップボックス、スマートフォンもしくはセル電話、タブレット PC、スマートテレビまたはその他のネットワークもしくはインターネットに接続された家電製品である、請求項 1_3 に記載のエンドユーザデバイス。

10

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、エンドユーザデバイスの分野に関し、より具体的にはサービスプロバイダネットワークとのプロードバンド接続経由で動作するカスタマ構内設備デバイスなどの、遠隔管理されたインターネット接続のエンドユーザデバイスに関する。

【背景技術】

【0002】

カスタマ構内設備 (CPE) デバイスは、例えば、住居用ゲートウェイ、ルータ、スイッチ、電話機、セットトップボックスなどである。住居用ゲートウェイは、今日ではカスタマの住居内のデバイスをインターネットまたはその他の広域ネットワーク (WAN) に接続するために広く使用されている。住宅用ゲートウェイは、例えば、銅線を介して高データレート伝送を可能にするデジタル加入者線 (DSL)、または例えば、ファイバー・トゥ・ザ・ホーム (FTTH) およびファイバー・トゥ・ザ・プレミシズ (FTTP) などの、光ファイバープロードバンド伝送システムを使用する。

20

【0003】

ネットワークサービスプロバイダ (NSP)、さらに一部のインターネットサービスプロバイダ (ISP) は、例えば、プロードバンドインターネットアクセスまたは IPTV のサービスの一環としてこれらのサービスプロバイダが設置した数百万にものぼる大量の CPE デバイスを管理しなければならない場合もある。CPE デバイスの遠隔管理は、個々の CPE デバイスと対話してこれらのデバイスにコンフィギュレーション設定を提供し、そして特定のアプリケーション層プロトコルを使用して診断情報を抽出する、中央コンフィギュレーションサーバ (CCS) によって実現することができる。

30

【0004】

広く使用されている CPE 遠隔管理通信プロトコルの例として、CPE WAN 管理プロトコル (CWMP) が知られており、そのプロトコルは、プロードバンドフォーラムによって発展したものであり、技術レポート番号 069 で規定され、一般に TR-069 とも呼ばれている。CWMP は、CPE デバイスと自動コンフィギュレーションサーバ (ACS) との通信プロトコルを設けることによって、CPE デバイスを遠隔管理するアプリケーション層プロトコルを規定している。

40

【0005】

CPE デバイスにプロードバンドサービスを提供するこの種の広域ネットワークは、図 1 に概略的に示されている。即ち、ネットワークサービスプロバイダネットワーク 1 は、インターネットサービスを例えば、DSL / ケーブル / ファイバーなどのプロードバンド接続 5 経由で多数の住居用ゲートウェイ 2 およびセットトップボックス 3 に提供するために用意されている。さらに、NSP ネットワーク 1 は、住居用ゲートウェイ 2 およびセットトップボックス 3 を遠隔管理する ACS 4 を含む。TR-069 プロトコルの使用により、ACS 4 は、例えば、自動コンフィギュレーションおよび動的なサービスプロビジョニング、ソフトウェア / フームウェア画像の管理、住居用ゲートウェイ 2 およびセットトップボックス 3 のステータスおよび性能のモニタリングおよび診断を行う能力を有する。

50

【0006】

C W M P 、さらに例えば、 O M A デバイスマネジメント(OMA Device Management)またはウェブサービスベースのプロトコルなどの、他のプロトコルは、「従来の」クライアント / サーバおよび要求 / 応答モデルにおいて機能する。 H T T P (Hypertext Transfer Protocol) のクライアントとして機能するデバイスは、 1 または一群の H T T P サーバに接続して H T T P リクエストを送信し、そして 1 または一群のサーバは、 H T T P 応答で応答する。 C W M P は、それに応じてワールドワイドウェブ(World Wide Web) サービングウェブ(H T M L) ページと同じプリンシバルを適用する。

【0007】

最近では、 <http://www.w3.org/TR/htm15/> を参照すればわかるように、最新の(upcoming) H T M L 5 標準の範囲において進化が見られ、 W 3 C の寄与による規定：“ <http://tools.ietf.org/html/draft-ietf-hybi-thewebsocketprotocol-17> ” に従った新しいウェブソケットプロトコルが存在する。ウェブソケットは、ウェブソケットクライアントとウェブソケットサーバとの全二重双方向通信をサポートし、従来の要求 / 応答モデルを上回るが、サーバがデータをクライアントに送信するための中間非標準機構が存在し、その例は、コメット(comet)：<http://svn.cometd.com/trunk/bayeux/bayeux.html> 、 h t t p ロングポーリングなどを含む。

【0008】

管理に関連するロジックおよび H T T P 要求 / 応答モデルのすべてを含む完全に集中化されたサーバに対する重大な制約および問題がいくつかある。即ち、

- 集中サーバモデルにおいて、数百万のデバイスが（リクエストを送信する）サーバに頻繁に接続すると、ヘルプデスクおよび他のエンティティがサーバのいくつかのアプリケーション（モニタリング、診断など）を処理しなければならないことからスケーラビリティが課題となる。

- A C S または他のバックエンドアプリケーションから特定のデバイスにできるだけ高速に通信することは厄介である。例えば、 TR - 0 6 9 は、 A C S が H T T P リクエストを C P E に送信する接続要求機構を規定し、典型的には H T T P ダイジェスト認証を使用して認証し、その後 C P E デバイスが、 H T T P リクエストを送信する A C S に接続する。

- 多数の C P E デバイスの問い合わせ(interrogation)では、中央サーバが各デバイスとコンタクトし、要求 / 応答の反復を個々に処理してデータを収集し、そしてこれらの収集データをサーバ側で分析する必要がある。

- すべてのロジックは、一つの場所、例えば、 A C S サーバに集中化され、以下のようになる。

A C S サーバは、潜在的に低速なネットワーク接続を介してコマンドをデバイスに送らなければならない。

A C S サーバは、 C P E デバイスからの応答（成功 / 失敗および見込まれる必要なデータ）を待ち、この結果を分析し、そしてこの結果に基づいて次に取るべきステップを決定しなければならない。

典型的には、膨大な数の C P E デバイスに共通であるこのロジックを個々の C P E デバイスに実行する。

【0009】

特許文献 1 では、広域ネットワーク経由でさまざまなユーザ宅内のゲートウェイデバイスと通信し、ゲートウェイデバイスと関連するカスタマのサービスサブスクリプションに基づいて、ゲートウェイデバイスによるアプリケーションサービスおよび / またはフィーチャの配信を遠隔管理する、サービス管理システムが説明されている。サブスクリプションマネージャは、 W A N を介して使用可能なアプリケーションサービスまたはフィーチャを特定する情報をそれぞれのゲートウェイデバイスに提供する。サブスクリプションマネージャによって制御されるサービスマネージャは、ゲートウェイデバイスからのリクエストに応答して、ゲートウェイデバイスのアプリケーションサービスにサービス機能性を実

10

20

30

40

50

装するロジックにサービス専用のコンフィギュレーションデータを配布する。

【0010】

非特許文献1では、ネットワーク管理のアプリケーション設計が説明されている。第1に、プルモデルは、要求／応答パラダイムに基づいている。第2に、プッシュモデルは、アドミニストレータがネットワーク帯域幅ならびにCPU時間を管理局で保存できるようになるにさせる、パブリッシュ／サブスクリープトパラダイムに依存している。第3のモデルは、上記2つのモデルが共存する、折り畳み式の(collapsed)ネットワーク管理プラットフォームの概念を導入している。

【先行技術文献】

【特許文献】

10

【0011】

【特許文献1】米国特許出願公開第2010/0235433

【非特許文献】

【0012】

【非特許文献1】“Push vs. Pull in WEB-Based Network Management” by Jean-Philippe Martin-Flatin, Lausanne, Switzerland, Technical Report SSC/1998/022

【発明の概要】

【0013】

本システムは、ブロードバンド接続経由でサービスプロバイダネットワークに結合された多数のエンドユーザデバイスと、多数のエンドユーザデバイスと通信するように適合されたパブリッシュ／サブスクリープトプローカと、サービスプロバイダネットワークに結合された少なくとも第1のバックエンドエンティティと、を備える。第1のバックエンドエンティティは、パブリッシュ／サブスクリープトプローカに接続して、エンドユーザデバイスのデバイス管理を行うために制御データチャネル経由で制御データをパブリッシュする、第1のクライアントソフトウェアアプリケーションを含む。エンドユーザデバイスのそれぞれは、パブリッシュ／サブスクリープトプローカに接続し、制御データチャネルをサブスクリープトし、制御データを受信し、そしてさらに制御データによる指示に応じてデバイスデータおよびアクションデータをパブリッシュする、第2のクライアントソフトウェアアプリケーションを含む。バックエンドエンティティの承認は、具体的には制御データ署名を使用することによって確認される。

20

【0014】

好適な実施形態において、サービスプロバイダネットワークは、インターネットサービスを、例えば、ネットワークサービスプロバイダネットワークに提供し、エンドユーザデバイスのデバイス管理を提供するネットワークであり、そしてパブリッシュ／サブスクリープトプローカも、ネットワークサービスプロバイダネットワークを運用するネットワークサービスプロバイダによって提供される。各エンドユーザデバイスは具体的には、そのデバイス管理を行う管理コマンドを受信するために少なくとも1つの制御データチャネルをサブスクリープトし、そして各エンドユーザデバイスは、そのデバイスデータをデバイスデータチャネル経由でパブリッシュし、アクションデータをアクションデータチャネル経由でパブリッシュする。

30

【0015】

本発明のさらなる態様において、システムは、パブリッシュ／サブスクリープトプローカに接続する第3のクライアントソフトウェアアプリケーションを有する第2のバックエンドエンティティを含み、プローカは、多数のエンドユーザデバイスのインベントリを保持するためにエンドユーザデバイスのデバイスデータ、制御データおよびアクションデータをサブスクリープトするが、エンドユーザデバイスの制御データはパブリッシュしない。第2のバックエンドエンティティは、例えば、エンドユーザデバイスのメーカーによって提供されるサーバであり、第1のバックエンドエンティティは、ネットワークサービスプロバイダによって提供されるサーバである。

40

【0016】

50

デバイス管理は具体的には、新しいファームウェアまたはミドルウェアバージョンへのアップグレードを行い、ソフトウェアアプリケーションのインストール、更新またはアンインストールを行い、プログラムまたはスクリプトファイルを実行し、エンドユーザデバイスのコンフィギュレーションまたはステータスデータに対する構造化クエリを実行し、どのデータをエンドユーザがパブリッシュする必要があるか、またはエンドユーザデバイスのリセットまたはリポートについてのポリシーを提供することを含む。

【0017】

システムと動作するように適合されたエンドユーザデバイスは、具体的にはCPEデバイスであり、例えば、住居用ゲートウェイおよびセットトップボックス、さらにスマートフォン、セル電話、タブレットPC、スマートテレビ、および他の遠隔管理されたネットワークまたはインターネット接続の家電製品である。

10

【図面の簡単な説明】

【0018】

本発明の好適な実施形態は、概略図を参照し、例として以下により詳細に説明される。
【図1】CPEデバイス、およびインターネットサービスを提供するネットワークサービスプロバイダネットワークを含む、先行技術に係る広域ネットワークの図である。

【図2】本発明に係る多数のエンドユーザデバイス、パブリッシュ／サブスクライブプロトコル、および2つのバックエンドエンティティを備えるシステムの図である。

【図3】図2のシステムの好適な実施形態の図である。

【図4】図2および図3に示されたようにバックエンドエンティティの実行アクションを実行する方法の図である。

20

【図5】図3に示されたようにシステムの例示的なオペレーション方法を説明する図である。

【発明を実施するための形態】

【0019】

以下の記載において、ブロードバンド接続経由でサービスプロバイダネットワークに結合された多数のエンドユーザデバイスを備えるシステムが説明されている。説明を目的として、好適な実施形態への完全な理解を与えるために、多数の具体的な詳細が示されている。しかしながら、本発明がそのような具体的な詳細を用いずに実施され得ることは当業者には明らかである。

30

【0020】

エンドユーザデバイスは、具体的にはCPEデバイスであり、例えば、住居用ゲートウェイ、ルータ、スイッチおよびセットトップボックス、さらにその他のネットワークまたはインターネット接続の家電製品であり、そして各デバイスに、マイクロプロセッサ、オペレーティングシステムおよびアプリケーションが格納された不揮発性メモリ、およびCPRデバイスが動作するための揮発性メモリを含む。CPEデバイスのオペレーティングシステムは、例えば、LINUX(登録商標)オペレーティングシステムおよびCPEデバイス専用ミドルウェアであり、ミドルウェアは、デバイス実行環境を表す。デバイス実行環境は、例えば、DSLモデム機能を提供するソフトウェアコンポーネント、ゲートウェイおよびスイッチング機能、FXS機能、VOIP機能性およびWi-Fiオペレーションを含む。

40

【0021】

本発明に係るシステムは、図2に示された好適な実施形態において、各デバイスがブロードバンド接続13経由でサービスプロバイダネットワーク10、具体的にはネットワークサービスプロバイダ(NSP)ネットワークに結合された多数のCPEデバイス12、および多数のCPEデバイスと通信するように適合されたパブリッシュ／サブスクライブプロトコル11を含む。システムは、ブロードバンド接続16経由でサービスプロバイダネットワークに結合された少なくとも第1のバックエンドエンティティ14を含み、バックエンドエンティティ14は、CPEデバイス12に遠隔CPEデバイス管理を行うパブリッシュ／サブスクライブプロトコル11に接続するクライアントソフトウェアアプリケーシ

50

ヨンを含む。パブリッシュ／サブスクライブプローカ 1 1 は、例えば、N S P ネットワーク 1 0 の一部であるかまたはインターネットサービスプロバイダによって提供され、具体的には C P E デバイス 1 2 に遠隔 C P E デバイス管理を行うために C P E デバイス 1 2 の通信および制御サービスを管理する。パブリッシュ／サブスクライブプローカ 1 1 は、N S P ネットワーク 1 0 またはインターネットサービスプロバイダネットワーク外部のデータセンタに配置されたクラウドプラットフォームにホストされることも可能である。C P E デバイス 1 2 は、パブリッシュ／サブスクライブプローカ 1 1 に接続しているクライアントソフトウェアアプリケーションも含み、従ってパブリッシュ／サブスクライブプローカ 1 1 およびバックエンドエンティティ 1 4 の「管理下にある」デバイスである。C P E デバイス 1 2 は、1 またはいくつかの特定のトピック、例えば、1 またはいくつかの制御チャネルをサブスクライブし、そして 1 またはいくつかの特定のトピック、例えば、データチャネルにデータをパブリッシュする。10

【 0 0 2 2 】

また、ブロードバンド接続 1 7 経由でパブリッシュ／サブスクライブプローカ 1 1 に接続されたさらなるバックエンドエンティティ 1 5 は、C P E デバイス 1 2 の C P E デバイス管理を提供またはサポートするためにパブリッシュ／サブスクライブプローカ 1 1 に接続するクライアントアプリケーションソフトウェアを含む。バックエンドエンティティ 1 4 および / または 1 5 は、具体的なアプリケーションまたはユースケースによって、特定のトピック、例えば、制御チャネルに制御データをパブリッシュし、そして特定のトピック、例えば、データチャネルをサブスクライブする。20

【 0 0 2 3 】

バックエンドエンティティ 1 4 および 1 5 を異なる技術、例えば、異なるソフトウェアプログラミング言語で実装し、そして同じサーバまたは異なるサーバおよび場所、例えば、インターネット接続性を有する世界中の任意の場所に配置することができる。他のデバイスと同様に、それらのエンティティは、パブリッシュ／サブスクライブプローカ 1 1 を介してインターネット上で通信する。本発明は具体的には、任意の場所に常駐する 1 、 2 、または任意の数のバックエンドエンティティをサポートする。

【 0 0 2 4 】

パブリッシュ／サブスクライブシステムにおいて、パブリッシャは、中間メッセージブローカ、パブリッシュ／サブスクライブプローカ 1 1 にメッセージをポストし、そしてサブスクライバは、そのプローカの登録サブスクリプションをサブスクライブし、プローカは、パブリッシュされたメッセージの転送およびフィルタリングを実行する。プローカは通常、格納を実行して、パブリッシャからサブスクライバへのメッセージをルートする機能ができるだけ効率的なやり方で転送するように最適化されている。メッセージプローカは、例えば、http://en.wikipedia.org/wiki/message_broker に説明されている。パブリッシュ／サブスクライブ機構は、疎結合されたエンティティ間で一対一、一対多および多対多通信を可能にする。疎結合とは、本発明の文脈においてエンティティが互いの存在またはロケーションについて知る必要がないことを意味する。プローカは、各クライアント、C P E デバイスまたはバックエンドエンティティを認証し、そしてメッセージが一部のチャネルにパブリッシュされるときに、どのバックエンドエンティティがどのメッセージをサブスクライブして受信することを許可されているかについての承認制約条件を課す。3040

【 0 0 2 5 】

パブリッシュ／サブスクライブ機構は、例えば、スケーラブルな高リアルタイム性能およびパブリッシャとサブスクライバ間で相互運用可能なデータ拡張を可能にする、オブジェクト管理グループ (O M G) によって提供されるデータ配布サービス (D D S) によっても使用される。別の例は、I B M によって出されたオープンプロトコル仕様である、M Q T T (Message Queue Telemetry Transport) プロトコルである。この発明は、特定のパブリッシュ／サブスクライブ技術に依存していない。

【 0 0 2 6 】

いくつかまたは任意の数のバックエンドエンティティ 1 4 、 1 5 は、各々がパブリッシュ50

ユ / サブスクライブプローカ 1 1 に接続するクライアントソフトウェアアプリケーションを有しており、このクライアントソフトウェアアプリケーションは、パブリッシュ / サブスクライブプローカ 1 1 を使用することによって C P E デバイス 1 2 を管理するために使用することができる。このソリューションは具体的には、T R - 0 6 9 C W M P プロトコルまたは O M A D M プロトコルなどの、現在の参照規格よりもスケーラブルで費用効率が良い。パブリッシュ / サブスクライブプローカ 1 1 は、例えば、P u s h e r http://pusher.com と同様のサービスを使用してもよく、P u s h e r は、ウェブアプリケーション、B e a c o n p u s h , http://beaconpush.com、P u b N u b , http://www.pubnub.com、M Q T T プローカまたは超大規模 D D S (Distributed Data Services) , http://www.omg.org/news/meetings/GOV-WS/pr/rte-pres/ultra-large-scale-dds.pdf にリアルタイム双方向機能性を迅速で容易かつ安全に付加するための簡易なホスト A P I である。10

【 0 0 2 7 】

本システムは以下のように動作する。

1 . 各 C P E デバイス 1 2 は、第 1 のステップにおいてウェブベースのパブリッシュ / サブスクライブインフラストラクチャ、パブリッシュ / サブスクライブプローカ 1 1 (ウェブベースとは、プローカがインターネット経由で到達可能であることを意味する) に接続する。

【 0 0 2 8 】

a . C P E デバイス 1 2 のスタートアップ時に各 C P E デバイス 1 2 上で稼動するクライアントソフトウェアアプリケーションは、例えば、T C P 、パブリッシュ / サブスクライブプロトコル経由で(事前に)構成された U R L (uniform resource locator)を使用することによってパブリッシュ / サブスクライブプローカ 1 1 への接続を確立する。クライアントソフトウェアアプリケーションは、認証を行って、パブリッシュ / サブスクライブプローカがクライアントアイデンティティを確認できるようにさせる T L S (Transport Layer Security) 証明書を提供しなければならない場合もある。20

【 0 0 2 9 】

b . C P E デバイス 1 2 は、そのデバイスデータを事前構成されたチャネル / トピック、例えば、デバイスデータチャネルにパブリッシュできる。

【 0 0 3 0 】

i . そのデバイスデータは具体的には、シリアルナンバー、ハードウェアバージョン、ソフトウェアバージョン、現在のパブリック(インターネット)IP アドレスなどを含む。30

【 0 0 3 1 】

i i . バックエンドエンティティ 1 4 、 1 5 のいずれもデバイスデータをサブスクライブでき、例えば、バックエンドエンティティは、C P E デバイスを結び付けるデバイスデータと一緒に格納している、バックエンドデバイスインベントリアプリケーションを備える。

【 0 0 3 2 】

i i i . デバイスデータは、特定のイベント時、例えば、スタートアップまたはソフトウェアバージョンまたは IP アドレスの任意の変更時に各 C P E デバイス 1 2 によって定期的にパブリッシュされ得る。40

【 0 0 3 3 】

c . C P E デバイス 1 2 は、1 または複数の制御チャネルまたはトピックをさらにサブスクライブする。

【 0 0 3 4 】

i . サブスクライブするチャネル / トピックは、事前に受信した制御データによって決定されるか、または他の基準によって決定されるかのいずれかで事前構成されている。

【 0 0 3 5 】

1 . チャネルサブスクリプションを N S P ごと、領域ごと、サブスクライバグループごとに行って、制御データが特定の領域内かまたは特定のサービスをサブスクライブす50

ると見込まれる、特定の N S P のカスタマをターゲットにすることができるようとする。

【0036】

2. チャネルサブスクリプションは、時間が経つと変更することができ、例えば、所与の C P E 製品（ハードウェアバージョン）およびソフトウェアバージョンを有する N S P カスタマは、アップグレードを指示する制御データの特定のチャネル／トピックをサブスクライブすることができる。例えば、住居用ゲートウェイまたはセットトップボックスデバイスは、< N S P - H W - S W > チャネルをサブスクライブできるので、そのチャネルにパブリッシュされた制御データがそれらの C P E デバイス 1 2 を新しいファームウェア／ソフトウェアバージョンにする、大規模なアップグレードを行うことができる。アップグレードした後、各 C P E デバイス 1 2 は、新しくアップグレードされた制御データをリスンして、< N S P - H W - S W 2 > チャネルをサブスクライブできる。

【0037】

3. 選択的なチャネル／トピックサブスクリプションを用いて、C P E デバイス 1 2 の大規模なセットは、特定の遠隔管理アプリケーションごとに区分されるので、パブリッシュされたデータは、C P E デバイス 1 2 の特定のセットを対象とすることができる。

【0038】

i i . パブリッシュ／サブスクライブプローラは、構成可能なポリシーに基づいて、C P E デバイス 1 2 が特定のチャネル／トピックをサブスクライブするのを拒否できる。
2. バックエンドエンティティ 1 4 および / または 1 5 は、制御データを特定の制御チャネルまたはトピックにパブリッシュする。

【0039】

a . 1 または複数のバックエンドエンティティ 1 4 、 1 5 は、制御データを特定の制御チャネルまたはトピックにパブリッシュすることができる。従来の集中化された C W M P サーバと違い、パブリッシュ／サブスクライブ機構は、疎結合された通信：一対一、一対多、多対多通信を可能にする。バックエンドエンティティ 1 4 、 1 5 を別個にすることによって、例えば、スケーラビリティに伴う中央ボトルネックを避けることができる。

【0040】

b . 各バックエンドエンティティ 1 4 、 1 5 は、ウェブパブリッシュ／サブスクライブインフラストラクチャ、パブリッシュ／サブスクライブプローラ 1 1 を認証して、パブリッシュ制御データが許可されるようにしなければならない場合もある。

【0041】

c . 制御データは、例えば、異なるデータフィールドを包含できるが、以下に限定されない：

i . ターゲット C P E デバイス：サブスクライブする C P E デバイスに制御アクションを適用しなければならない任意の制限である。この制限は、C P E デバイス特性のセットの形式、例えば、H W / S W バージョン、I P アドレス範囲など、またはサブスクリーバ特性の形式、例えば、p p p 認証情報のセット、V o I P 電話番号（範囲）、アクティブサービスなどで表現できる。

【0042】

i i . アクション：C P E デバイス 1 2 によって実行されるアクション。例示的なアクションは以下のものが含まれるが、これらに限定されない：

- 1 . ファームウェアのアップグレード
- 2 . アプリケーションのインストール／更新／アンインストール
- 3 . プログラムまたはスクリプトファイルの実行
- 4 . パブリッシュ：C P E デバイスデータまたは固定データをデバイスまたはデータチャネルまたはトピックに無条件でパブリッシュする

5 . クエリ：C P E コンフィギュレーションデータまたはステータスデータに対する構造化クエリを行う（クエリが、C P E デバイスによってパブリッシュされるデータが存在するという結果を有する場合のみ）

- 6 . リブート

10

20

30

40

50

i i i . U R L : ファイルを指し示す任意選択の U R L 。これは、特定のアクションのみに適用する場合があり、例えば、ファームウェアのアップグレードの場合、 U R L は、ダウンロードして適用するファームウェア画像を指し示し、アクションとして実行する場合、 U R L は、ダウンロードして実行するソフトウェアプログラムまたはスクリプトファイルを指し示す。

【 0 0 4 3 】

i v . データチャネル : アクションの結果をパブリッシュするチャネル / トピック名。任意選択で、従来の H T T P 要求 / 応答ウェブサービスを使用してアクションの結果データをパブリッシュする U R L でもよく、例えば、 H T T P P O S T は、この U R L に対して J S O N (JavaScript (登録商標) Object Notation) がエンコードされたデータを用いる。

【 0 0 4 4 】

v . タイミングに関する基準 : 例えば、任意のタイミング制限であるが、以下に限定されない :

1 . 循環アクションを実行する間隔、例えば、モニタリングする理由によるスクリプトの定期的な実行間隔において、 0 値は、一回限りで循環しないアクションを示し得る。

【 0 0 4 5 】

2 . 相対遅延、例えば、アクションを実行する前の、固定またはランダムな範囲の相対遅延

3 . アクションを実行する絶対時間範囲、例えば、同日の午前 2 時と午前 4 時の間
v i . セキュリティ署名 : メッセージの署名は、見込まれる多数のバックエンドエンティティ 1 4 および 1 5 に対する分散アプローチにおいて必要なレベルのセキュリティを提供する、本発明の主要な要素である。中央認証機関は、許可された機能性を包含する拡張フィールドをバックエンドエンティティのデジタル証明書、例えば、 X . 5 0 9 に付加し、バックエンドエンティティ自身の証明書で署名することにより、バックエンドエンティティにいくつかの管理機能性を実行する権利を付与する。クライアントデバイスは、中央認証機関証明書の公開鍵を埋め込み、受信したメッセージごとに、メッセージを署名した証明書が適切な管理権を有していて、中央認証機関によって署名されたかどうかを確認する。

3 . パブリッシュ / サブスクライブプローカ 1 1 にサブスクライブして、バックエンドエンティティ 1 4 、 1 5 のいずれかから制御データを受信する各 C P E デバイス 1 2 は、要求されるアクションを実行する :

a . 第 1 のステップでは、制御データの発信元、信頼性および整合性を検証する :

i . 制御データは、例えば、署名、制御データメッセージにハッシュ値が暗号化された非対称鍵を包含することができる。

【 0 0 4 6 】

i i . メッセージ (バックエンドエンティティに対応する) の署名に使用される証明書秘密鍵は、その拡張フィールドに適切な管理権を包含し、そして C P E デバイス 1 2 に格納された中央認証機関の事前に準備された (pre-provisioned) 秘密鍵を使用して確認される。

【 0 0 4 7 】

b . 第 2 のステップでは、 C P E デバイス 1 2 が実際にアクションを実行すべきかどうかを評価する任意のターゲット C P E デバイス制約を確認する。 C P E デバイス 1 2 がターゲット制約の適用を受けていなければ、制御データメッセージは、それ以上のアクションを持たずに廃棄される。

【 0 0 4 8 】

c . アクションは、一部の任意の制御データフィールドが重要であるか否かを決定する。 C P E デバイス 1 2 は、例えば、任意のタイミング制約を考慮に入れたアクションを実行するが、以下に限定されない :

10

20

30

40

50

1. ファームウェアのアップグレード：ファームウェア画像をロケーションURL（ロケーションURLは、スキーマとして使用されるプロトコルを包含する）においてダウンロードし、ファームウェアをフラッシュ／適用した後にデバイスをリブートする。

【0049】

2. アプリケーションのインストール／更新／アンインストール：URL、例えば、file://スキーマを用いて特定される、特定のアプリケーションをインストールまたはアンインストールするアプリケーションバイナリをデバイスにダウンロードする。

【0050】

3. プログラムまたはスクリプトファイルを実行する：URLロケーションにおいてプログラムまたはスクリプトファイルをダウンロードして、プログラムまたはスクリプトファイルを実行する。 10

【0051】

4. パブリッシュ：CPEデバイスデータまたは固定データをデバイスデータチャネルまたはトピックに無条件でパブリッシュする。

【0052】

5. クエリ：CPEデバイス12のCPEデバイスコンフィギュレーションまたはステータスデータへの構造化クエリ（クエリが、CPEデバイスによってパブリッシュされるデータが存在するという結果を有する場合のみ）。

【0053】

6. リブート：CPEデバイス12のウォームリセットまたはウォームリストート。 20
4. CPEデバイス12は、アクションの結果をアクションデータチャネルまたはトピックにパブリッシュすることができる。

【0054】

a. 例えば、データは、特定のアクションによって異なるが、以下に限定されない：
1. ファームウェアのアップグレード：結果データは、故障障害コードであってもよい。成功した場合、デバイスは、デバイスデータをリパブリッシュできる（ステップ1.b参照）。

【0055】

2. アプリケーションのインストール／更新／アンインストール：結果データは、成功表示または失敗表示になり得る。 30

【0056】

3. プログラムまたはスクリプトファイルを実行する：結果データは、プログラムまたはスクリプト実行の結果である任意のデータであってもよい。それらのデータは、例えば、モニタリングデータ、診断結果コード、特定のクエリの結果、集合データなどになり得る。

【0057】

4. パブリッシュ：CPEデバイスデータまたは固定データ
5. クエリ：クエリは、結果を有する場合と有しない場合があり、結果データは、例えば、CPEコンフィギュレーションデータおよび／またはステータスデータに対して実行される、実際のクエリによって異なり、例えば、ブロードバンドフォーラムTR-18.1i2データモデルなどの標準ゲートウェイデータモデルを参照する。 40

【0058】

6. リブート：例えば、リブートした後、結果データがなければCPEは、そのデバイスデータをリパブリッシュできる。

【0059】

b. データをパブリッシュするデータチャネルまたはトピックは、アクションをトリガした初期制御データによって決定される。

【0060】

i. 各アクションのデータチャネルまたはトピックは、異なることもあり、これは、制御データを管理するバックエンドアドミニストレータによって完全に決定される。 50

【 0 0 6 1 】

i i . 1 または複数のバックエンドエンティティ 1 4、1 5 が関心を示してアクションデータチャネルまたはトピックをサブスクライブすることもある。

5 . C P E デバイス 1 2 は、実行する新しいアクションを用いて、サブスクライブされる制御チャネルまたはトピックで新しい制御データを受信できる。

【 0 0 6 2 】

システムのより詳細な実施形態が図 3 に示されている。このシステムは、多数の C P E デバイス 1 2 および 1 8 を含み、それらのデバイスはそれぞれ、ブロードバンド接続 1 3 経由でサービスプロバイダネットワーク 1 0 とインターネットとに結合されている。システムは、パブリッシュ / サブスクライブプローカ 1 1 をさらに備え、そのプローカは、サービスプロバイダネットワーク 1 0 、例えば、N S P ネットワーク内に配置されるか、またはインターネット内のどこかに配置される。システムは、数百万の C P E デバイス 1 2 を含むことができ、各デバイスは、パブリッシュ / サブスクライブプローカ 1 1 との接続、C P E デバイス 1 2 の C P E デバイス管理を行うためのクライアントソフトウェアアプリケーションを有する。それぞれの C P E デバイス 1 2 は、パブリッシュ / サブスクライブプローカ 1 1 の 1 または複数の制御チャネル（複数）をサブスクライブし、そしてそれぞれの C P E デバイス 1 2 は、データチャネル、例えば、デバイスデータチャネルおよびアクションデータチャネルにパブリッシュし、それらのチャンネルを経由して、C P E デバイス 1 2 は、そのデバイスデータ、例えば、ハードウェアおよびソフトウェアデータ、I P アドレスなどを送信することができる。

【 0 0 6 3 】

システムは、第 1 および第 2 のバックエンドエンティティ 1 4、1 5 をさらに含み、それらのエンティティは、パブリッシュ / サブスクライブプローカ 1 1 にも接続されている。好適な実施形態において、バックエンドエンティティ 1 4、1 5 の両方は、C P E デバイス 1 2 のデータチャネルをサブスクライブして、どの C P E デバイス 1 2 がインストールされていて、現在アクティブであるかをそれらのエンティティが認識できるようにする。別の例示的な実施形態において、バックエンドエンティティ 1 4 のみがデバイスデータをサブスクライブする。なぜなら、そのエンティティは、単なる一例として、すべての C P E デバイス 1 2 のインベントリを保持し、C P E デバイス 1 2 の最も不可欠な情報、例えば、ハードウェアおよびソフトウェアデータ、C P E デバイス 1 2 がいつデータをパブリッシュしたか、どの制御データを実行したか、などのデータを格納するからである。バックエンドエンティティ 1 5 は、制御データチャネルおよびアクションデータチャネル経由でパブリッシュ / サブスクライブプローカ 1 1 に結合されている。制御データチャネル経由で、バックエンドエンティティ 1 5 は、U R L を含む実行アクションを C P E デバイス 1 2 に送信することができ、そこで U R L は、C P E デバイス 1 2 によって実行されるプログラムまたはスクリプトを指示する。

【 0 0 6 4 】

バックエンドエンティティ 1 4 は、パブリッシュ / サブスクライブプローカ 1 1 によって提供される、制御データチャネル、デバイスデータチャネルおよびアクションデータチャネルをサブスクライブして、バックエンドエンティティ 1 5 から制御データおよび C P E デバイス 1 2 のデバイスデータおよびアクションデータを受信する。

【 0 0 6 5 】

2 または多数のバックエンドエンティティがロジックまたは必要性に従ってどのようにチャネル / トピックおよびメッセージの一部またはすべてをサブスクライブするかについての例がある。特定のバックエンドエンティティは、特定のチャネル部をサブスクライブして、ある N S P 、ある領域などからのデバイスへパブリッシュのみ、または当該デバイスからメッセージの受信のみを行うことができる。バックエンドエンティティは、他のすべての機能性を維持しながらシステムに動的に付加されるまたは除去されることもできる。

【 0 0 6 6 】

10

20

30

40

50

上記の例において、CPEデバイス12は具体的には、パブリッシュ／サブスクライブプローカ11によって提供される制御データチャネルをサブスクライブし、そしてデバイスデータチャネルおよびアクションデータチャネル経由でパブリッシュ／サブスクライブプローカ11にパブリッシュする。CPEデバイス12は、従って、バックエンドエンティティ15によって提供される制御データチャネル経由で任意のアクションデータを受信し、制御データによる指示に基づいてプログラムまたはスクリプトをダウンロードして、それを実行する。プログラムまたはスクリプトを実行した後、CPEデバイス12は、アクションデータとしての結果をアクションデータチャネルにパブリッシュし、その情報は、パブリッシュ／サブスクライブプローカ11によって第1および第2のバックエンドエンティティ14、15に転送される。バックエンドエンティティ15は、例えば、ネットワークサービスプロバイダのサーバであり、CPEデバイス12のアクションの進行を追跡する制御データを使用する。また、バックエンドエンティティ14は、例えば、CPEデバイス12のベンダーのサーバであり、CPEデバイス12のオペレーションを追跡して、CPEデバイス12がアクションを完了した情報を格納する。

【0067】

CPEデバイス18は、デバイスデータチャネル経由でデバイスデータのみをパブリッシュ／サブスクライブプローカ11にパブリッシュする。なぜならば、CPEデバイス18は、異なるネットワークサービスプロバイダに属し、バックエンドエンティティ15によって制御されていないからである。CPEデバイス12は具体的には、同じネットワークサービスプロバイダによって提供され、および／またはNSPネットワークの一部である。

【0068】

第1のバックエンドデバイス15の実行アクションを経由して、例えば、新しいソフトウェアアプリケーションをCPEデバイス12にインストールすることができ、またはファームウェアのアップデートをCPEデバイス12に実行することができる。バックエンドエンティティ15の実行アクションを実行する方法について、バックエンドエンティティ15とCPEデバイス12との間のデータフローを示した図4と関連して概略的に説明する。バックエンドエンティティ15は、CPEデバイス12の制御データを制御データチャネル経由でパブリッシュ／サブスクライブプローカ11にパブリッシュし、パブリッシュ／サブスクライブプローカは、例えば、URLを含む実行アクションを送信することによってその制御データをCPEデバイス12に転送する（ステップ20）。実行アクションは、例えば、以下の種類のJSON（JavaScript（登録商標）Object Notation）メッセージである：

```
{"ctrl": {"action": "exec", "key": 45335435, "url": "https://username:password@tchbackend.com/files/sdghsdg.lua", "data": "dsdghf321", "target": "*"}, "signature": "<base64encoded signature over ctrl data>"}。JSONは、メッセージを直列化するほんの一例であり、他の例は、XML（Extensible Markup Language）、ASN.1、CSV（Comma Separated Values）を含むが、これらに限定されない。
```

【0069】

次のステップ21において、CPEデバイス12は、JSONファイルにおいて指示されURLにおいて位置が特定されるスクリプトファイルをダウンロードする。スクリプトファイルは、例えば、Luaスクリプトファイルである。CPEデバイス12は、スクリプトファイルに含まれている制御データの署名の有効性を確認し、そしてその署名が信頼のあるバックエンド秘密鍵によって署名されたかどうかを確認する。有効性の確認には、基本的識別またはダイジェストの識別、例えば、ユーザ名およびパスワードが、HTTP

Getコマンドを使用して、http経由でURL：<https://tchbackend.com/files/sdghsdg.lua>から要求される。

【0070】

有効な秘密鍵および署名の場合、CPEデバイス12は、このスクリプトを実行する（ステップ22）。スクリプトは、任意の条件付きまたは無条件の対話、例えば、コンフィ

ギュレーションを変更し、状態または統計をチェックし、統計を読み出してそれを合計するかまたはそれを警告閾値でチェックするなどを実行することができる。スクリプト結果は、例えば、成功、詳細な故障コードを含む失敗表示、状態 / 統計、特定のクエリ結果であるかまたは含むことができ、そしてアクションデータチャネルのアクションデータとしてパブリッシュ / サブスクライブプローカ 1 1 にパブリッシュされ、パブリッシュ / サブスクライブプローカは、その結果をバックエンドエンティティ 1 5 に転送する（ステップ 2 3）。

【 0 0 7 1 】

図 3 と関連して説明したシステムの例示的なオペレーションを図 5 と関連して説明する。第 1 の C P E デバイス 1 2 _ c l i e n t 1 は、そのデバイスデータをパブリッシュ / サブスクライブプローカ 1 1 にパブリッシュする（ステップ 3 0）。パブリッシュ / サブスクライブプローカ 1 1 は、 d e v i c e 1 データを第 1 のバックエンドエンティティ 1 4 _ b a c k e n d 1 および第 2 のバックエンドエンティティ 1 5 _ b a c k e n d 2 に転送する（ステップ 3 1、3 2）。ステップ 3 3 において、第 2 の C P E デバイス 1 2 _ c l i e n t 2 は、そのデバイスデータをパブリッシュ / サブスクライブプローカ 1 1 にパブリッシュし、パブリッシュ / サブスクライブプローカは、 d e v i c e 2 データをそれに対応して b a c k e n d 1 サーバ 1 4 および b a c k e n d 2 サーバ 1 5 に転送する（ステップ 3 4、3 5）。さらに、 C P E デバイス 1 8 _ c l i e n t 3 は、そのデバイスデータをパブリッシュ / サブスクライブプローカ 1 1 に転送し、パブリッシュ / サブスクライブプローカは、これらのデバイスデータを b a c k e n d 1 バックエンドエンティティ 1 4 および b a c k e n d 2 バックエンドエンティティ 1 5 に転送する（ステップ 3 6 ~ 3 8）。バックエンドエンティティ 1 5 は具体的には、ネットワークサービスプロバイダのサーバであり、バックエンドエンティティ 1 4 は、 C P E デバイス 1 2 のベンダーのサーバである。ステップ 3 9 において、 d e v i c e 1 ~ d e v i c e 3 のデバイスデータは、サーバ 1 4 , 1 5 によって ログに記録される。

【 0 0 7 2 】

次のステップ 4 0 において、 b a c k e n d 2 サーバは、制御アクションを開始して、制御データをパブリッシュ / サブスクライブプローカ 1 1 にパブリッシュする（ステップ 4 1）。パブリッシュ / サブスクライブプローカ 1 1 は、これらの制御データを c l i e n t 1 C P E デバイスおよび c l i e n t 2 C P E デバイスに転送するが（ステップ 4 2、4 3）、 c l i e n t 3 C P E デバイスには転送しない。制御データもパブリッシュ / サブスクライブプローカ 1 1 によって b a c k e n d 1 サーバ 1 4 に転送され、このサーバは、制御データをログに記録する（ステップ 4 4、4 5）。ステップ 4 6、4 7 において、制御データは c l i e n t 1 C P E デバイスおよび c l i e n t 2 C P E デバイスによって処理され、実行される（ステップ 4 6、4 7）。 c l i e n t 1 デバイスがアクションを終了したとき、このデバイスは、アクションデータをパブリッシュ / サブスクライブプローカ 1 1 にパブリッシュし（ステップ 4 8）、パブリッシュ / サブスクライブプローカは、アクションデータを b a c k e n d 1 サーバ 1 4 および b a c k e n d 2 サーバ 1 5 に転送する（ステップ 4 9、5 0）。 c l i e n t 2 デバイスが終了してアクションを実行したとき、このデバイスは、そのアクションデータをパブリッシュ / サブスクライブプローカ 1 1 にパブリッシュし、パブリッシュ / サブスクライブプローカは、アクションデータを b a c k e n d 1 サーバ 1 4 および b a c k e n d 2 サーバ 1 5 に転送する（ステップ 5 1 ~ 5 3）。アクションデータは、 b a c k e n d 1 サーバおよび b a c k e n d 2 サーバによって ログに記録され（ステップ 5 4）、その後、実行アクションおよび制御が完了する（ステップ 5 5）。

【 0 0 7 3 】

図 3 と関連して説明されたシステムは、従ってパブリッシュ / サブスクライブプローカ 1 1 と多数の C P E デバイス 1 2 と 1 またはいくつかのバックエンドエンティティ 1 4 , 1 5 との間で一対一、一対多、多対多通信を可能にする。バックエンドエンティティ 1 4 , 1 5 は、具体的には N S P ネットワーク 1 0 のネットワークサービスプロバイダによつ

10

20

30

40

50

て、任意のインターネットサービスプロバイダによって、または CPE デバイス 12 のベンダーまたはメーカーによって提供および / または管理されるサーバである。バックエンドエンティティ 15 は、例えば、ネットワークサービスプロバイダによって提供されるサーバであり、バックエンドエンティティ 14 は、CPE デバイス 12 のメーカーによって提供されるサーバである。

【 0074 】

本発明は、一つの特定のパブリッシュ / サブスクライブ技術に頼るのではなく、見込まれる多数のバックエンドエンティティによるエンドユーザデバイス管理の発明概念を加えることで、今日の業界の参照プロトコルよりもスケーラブルで費用効率が良い代替的な総合的ソリューションを提供する。

10

【 0075 】

本システムは、以下の利点を有する：このアプローチは、例えば、通信オーバーヘッド、バックエンドエンティティがサポートすることができるデバイスの数に関して、従来の集中化された要求 / 応答ベースの管理アプローチよりもスケーラブルである。それによってバックエンドエンティティが中央 ACS に依存する必要がなくなる。さらに、このアプローチは、エンドユーザデバイスとバックエンドエンティティとの一対一、一対多および多対多通信を疎結合された形式でサポートし、デバイスとエンティティがどこにでも常駐できる。

【 0076 】

本システムは、さらに高速のバックエンド - デバイス間通信をサポートする。なぜならば、ACS は最初に接続要求を CPE デバイスに送信しなければならず、その後で CPE デバイスが管理セッションを行うために ACS に接続するという事例を有する、TR - 069 のような既存のソリューションに比べ、バックエンドエンティティは、データを常時送信 / パブリッシュすることができるからである。このシステムによって、典型的には CPE デバイス自体から多数の CPE デバイスに適用されるバックエンドロジックを配布することがさらに可能になり（集中化された TR - 069 ACS ロジックに対し）、スケーラビリティがかなり改善する。なぜならば、中央場所へ費用のかかる通信を行う必要がなくなるからである（典型的には ACS ロジックは、デバイス上でデータを取り出すかまたは更新し、その結果 / 成果に基づいて次のステップをとる）。

20

【 0077 】

本システムはさらに、従来の中央サーバが、例えば、ACS をサポートするのと違い、任意の数のバックエンドエンティティをサポートし、そして現在の最高水準（TR - 069、SNMP、OMA - DM）と比べて非常に広範囲の管理アプリケーションをサポートする。本システムは、（集中化されたブローカ、マルチキャストベースのパブリッシュ / サブスクライブプロトコルなどを用いて）下層の任意のウェブパブリッシュ / サブスクライブインフラストラクチャもサポートする。CPE デバイス 12 は、具体的には小規模なデータ配布サービスに基づいてオペレーションを行う、ミドルウェアを使用できる。この種のミドルウェアは、パブリッシュ / サブスクライブ機構を経由してパブリッシュ / サブスクライブプロトコル 11 と動作するように容易に適用される。

30

【 0078 】

さらに本発明の他の実施形態は、本発明の範囲から逸脱することなく当業者によって利用されてもよい。本発明は、具体的には XDSL、DOCSIS またはファイバー伝送を使用したワイドエリアネットワークであり、その他の有線または無線ブロードバンド技術、例えば、テレビ分配ケーブル、任意の光伝送、電力線ブロードバンド、WiMax または 3G 無線接続性にも適用可能であるが、これらに限定されない。説明したように本システムは、具体的には CPE デバイス、例えば、住居用ゲートウェイ、ルータ、スイッチ、電話機およびセットトップボックス、および家電機器、例えば、セル電話またはスマートフォン、タブレット PC、およびスマートテレビなどの、あらゆる種類のネットワーク接続のエンドユーザデバイスに使用され得る。本発明は、従って以下に添付された本明細書の特許請求の範囲に属する。

40

50

本発明は以下の態様を含む。

(付記 1)

ブロードバンド接続経由でサービスプロバイダネットワーク(10)に結合された複数のエンドユーザデバイス(12)を備えるシステムであって、

前記システムは、前記複数のエンドユーザデバイス(12)と通信を行うように適合されたパブリッシュ／サブスクライブプローカ(11)および前記サービスプロバイダネットワーク(10)に結合された少なくとも第1のバックエンドエンティティ(14、15)をさらに備え、前記第1のバックエンドエンティティ(14、15)は、前記パブリッシュ／サブスクライブプローカ(11)に接続するためおよび前記エンドユーザデバイス(12)のデバイス管理を行うために制御データチャネル経由で制御データをパブリッシュする第1のクライアントソフトウェアアプリケーションを含み、10

前記エンドユーザデバイス(12)は、前記パブリッシュ／サブスクライブプローカ(11)に接続して前記制御データチャネルをサブスクライブし前記制御データを受信するため、および前記制御データによる指示に基づいてデバイスデータおよびアクションデータをパブリッシュするための第2のクライアントソフトウェアアプリケーションを含む、前記システム。

(付記 2)

前記第2のクライアントソフトウェアアプリケーションは、それぞれのエンドユーザデバイスのスタートアップ時に各エンドユーザデバイス(12)上で開始され、および事前構成されたユニフォームリソースロケータを使用することによって前記エンドユーザデバイスの前記パブリッシュ／サブスクライブプローカ(11)への接続を確立する、付記1に記載のシステム。20

(付記 3)

前記サービスプロバイダネットワーク(10)は、インターネットサービスを提供するための、および前記エンドユーザデバイスの前記デバイス管理を提供する、ネットワークサービスプロバイダネットワークである、付記1または2に記載のシステム。

(付記 4)

前記パブリッシュ／サブスクライブプローカ(11)は、前記ネットワークサービスプロバイダネットワークを運用するネットワークサービスプロバイダによって提供される、付記3に記載のシステム。30

(付記 5)

前記パブリッシュ／サブスクライブプローカ(11)は、インターネットサービスプロバイダによって提供される、付記1、2または3に記載のシステム。

(付記 6)

各エンドユーザデバイス(12)は、そのデバイス管理を行う実行コマンドを受信するための少なくとも1つの制御データチャネルをサブスクライブし、および各エンドユーザデバイス(12)は、デバイスデータチャネル経由で前記デバイスデータをパブリッシュし、およびアクションデータチャネル経由でアクションデータをパブリッシュする、付記1から5のいずれか1つに記載のシステム。

(付記 7)

前記パブリッシュ／サブスクライブプローカ(11)に接続する第3のクライアントソフトウェアアプリケーションを含む第2のバックエンドエンティティ(14)を備え、前記第2のバックエンドエンティティ(14)は、前記複数のエンドユーザデバイス(12)のインベントリを保持するために前記エンドユーザデバイス(12)のデバイスデータ、制御データおよびアクションデータをサブスクライブするが、前記エンドユーザデバイス(12)の制御データはパブリッシュしない、付記1から6のいずれか1つに記載のシステム。

(付記 8)

前記第2のバックエンドエンティティ(14)は、前記エンドユーザデバイス(12)のメーカーまたはベンダーによって提供されるサーバである、付記7に記載のシステム。50

(付記 9)

前記第1のバックエンドエンティティ(15)は、前記ネットワークサービスプロバイダによって提供されるサーバである、付記4に記載のシステム。

(付記 10)

前記エンドユーザデバイスの管理は、新しいファームウェアもしくはミドルウェアバージョンへのアップグレード、ソフトウェアアプリケーションのインストール、アップデートもしくはアンインストール、プログラムもしくはスクリプトファイルの実行、前記エンドユーザデバイス(12)のコンフィギュレーションもしくはステータスデータに対する構造化クエリの実行、または前記エンドユーザデバイス(12)のリセットもしくはリブートを含む、付記1から9のいずれか1つに記載のシステム。 10

(付記 11)

前記エンドユーザデバイスは、制御データ署名によりバックエンドエンティティの承認の有効性を確認する、付記の1から10のいずれか1つに記載のシステム。

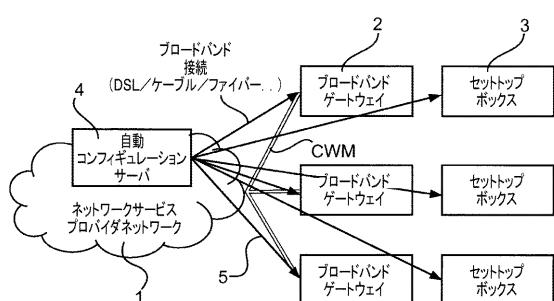
(付記 12)

付記1から11のいずれか1つに記載のシステムとオペレーションを行うように適合されたエンドユーザデバイス(12)。

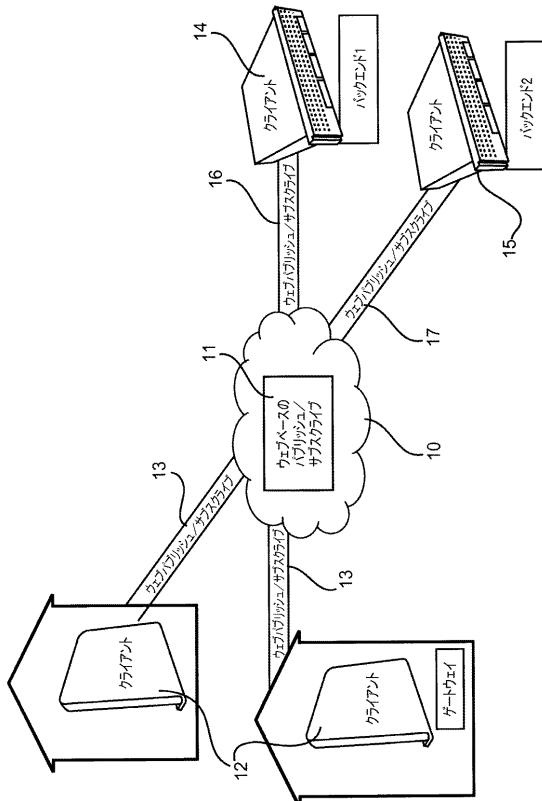
(付記 13)

前記エンドユーザデバイス(12)は、住居用ゲートウェイ、セットトップボックス、スマートフォンもしくはセル電話、タブレットPC、スマートテレビまたはその他のネットワークもしくはインターネットに接続された家電製品である、付記12に記載のエンドユーザデバイス。 20

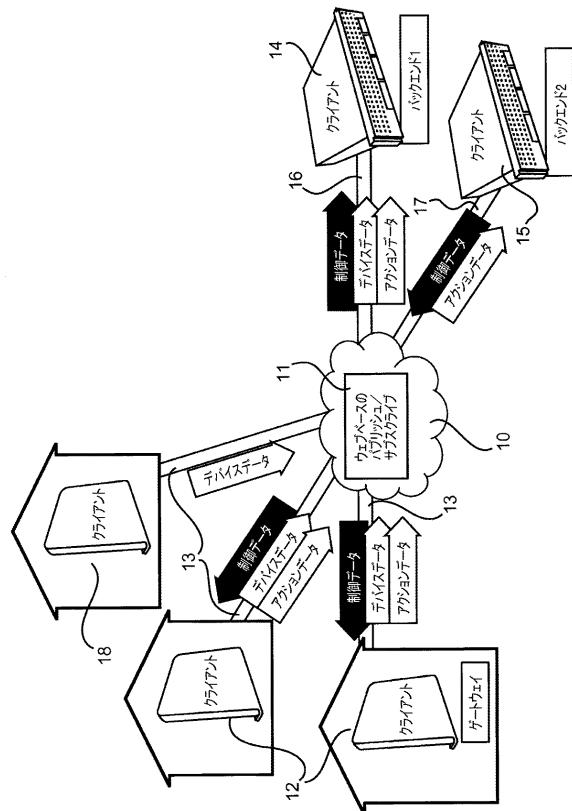
【図1】



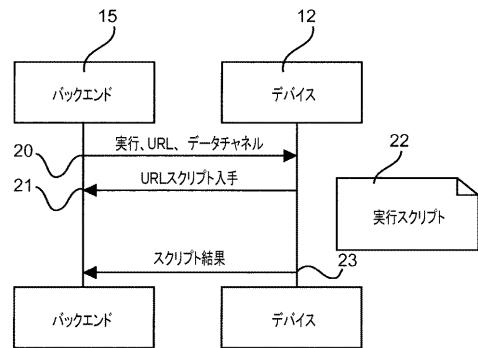
【図2】



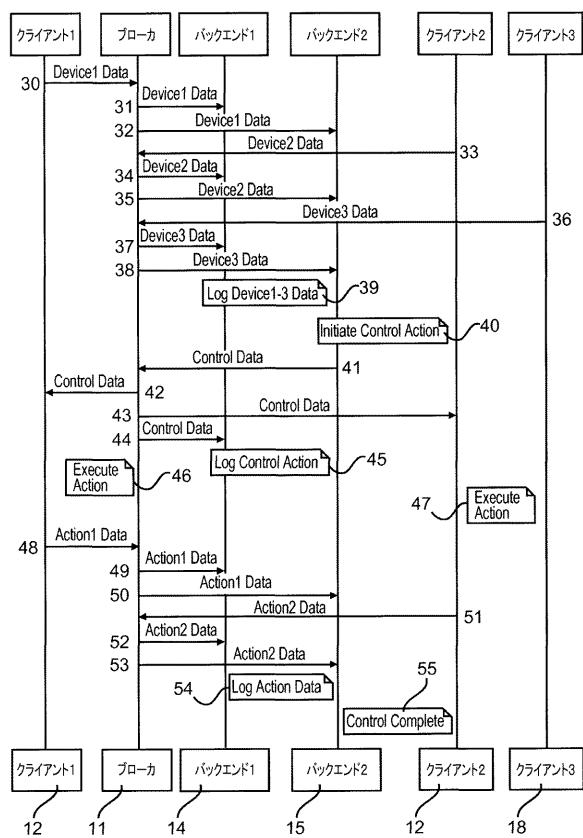
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者 ダーク ヴァン デ ポール
ベルギー 2650 エデゲム プリンス ボウドレンラーン 47 テクニカラー デリバリー
テクノロジーズ ベルギー内

(72)発明者 パトリック ゴエマエレ
ベルギー 2650 エデゲム プリンス ボウドレンラーン 47 テクニカラー デリバリー
テクノロジーズ ベルギー内

(72)発明者 カート ヨンキー
ベルギー 2650 エデゲム プリンス ボウドレンラーン 47 テクニカラー デリバリー
テクノロジーズ ベルギー内

審査官 佐々木 洋

(56)参考文献 米国特許第6718376(US, B1)
特開2006-352662(JP, A)
特開2009-223403(JP, A)
特開2004-348680(JP, A)

(58)調査した分野(Int.Cl., DB名)

G06F 13/00