

IoTのコストを低減する 組み込み機器向け接続基盤「NetNucleus Cloud Hub」

IoTの導入・運用には、遠隔監視・制御やセキュリティなどにおけるさまざまな課題が付きものです。(株)東芝 研究開発センターでは、これらの課題を解決しながらコスト低減も実現するWebベースのクラウド基盤技術を研究しています。この技術を当社にて「NetNucleus Cloud Hub」^{ネットニュークリアス クラウド ハブ}として商品化しました。今後、パッケージの提供などにより、お客様のIoTのスムーズな運用実現の支援を加速していきます。

本格運用を妨げる数多くの課題

IoT(Internet of Things)という言葉の示す範囲は幅広いものがあります。さまざまなデバイスやセンサーがネットワークで繋がり、そのデータを収集して見える化する、またデバイスの制御やデータの分析を行うことなどもIoTサービスの範疇と言えるでしょう。

当社が商品化したIoTクラウド基盤「NetNucleus Cloud Hub」は、その中核となる部分、即ち、デバイスとクラウドを接続する基本機能を提供するものです。デバイスとクラウドを接続するだけであれば、現在では容易に実現できるようになっていると思われるかもしれませんが、本格的に運用しようとするれば、さまざまな問題や壁があり、実現はそれほど容易なものではありません。

一例として、計測機器のアフターサービスでの運用を考えてみましょう。計測機器メーカーのサービス要員がエンドユーザに納入した多数の計測機器の稼動ログや計測値をネット経由で監視し、問題が発生したときは必要に応じてメンテナンスのための制御を行うというケースを考えると、基本機能だけでも次のような点が問題として浮上してきます。

●遠隔監視・制御

エンドユーザのネットワーク網の中に配備された計測機器は容易に制御できない。通知や制御のリアルタイム性をいかに確保するか、といった問題に直面する。

●ユーザ・機器管理とセキュリティ

各々のサービス要員やエンドユーザがどの機器にどこまでアクセスできるのか、セキュリティや情報漏えいの問題を解決しなければ

ならない。

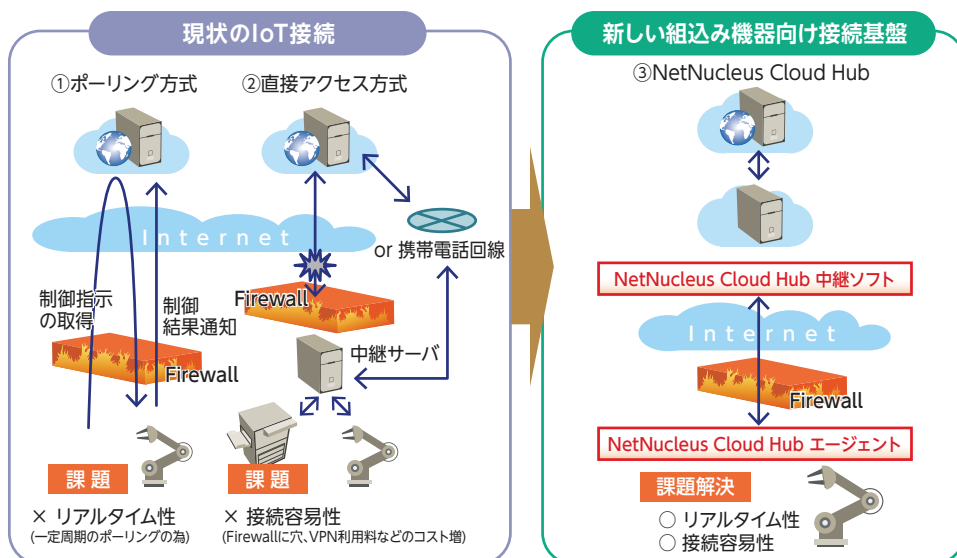
このほか、可用性とスケーラビリティの問題もあります。こうした問題を解決しながら、かつ開発コストやサービス運用・維持コスト、設置など導入コストをいかに抑えていくかといったことが要求されます。

接続調停アーキテクチャの採用による 大規模化への対応

こうした課題を解決するソリューションに取り組んできた当社が、お客様に提供するのが今回のNetNucleus Cloud Hubです。

(1) 接続の容易性とリアルタイム性

工場、ビルなどで遠隔監視・制御の対象となる多くの機器はローカルネットワークの中にあり、FirewallやNAT(Network Address Translation)の配下にあるため直接外部からアクセスできない、といった問題があります。ローカルネットワークの入口に専用のゲートウェイを個別に設置していくのはコストもかかり、かつ困難な場合もあります。さらに、監視・制御のリアル



タイム性の確保も不可欠です。

こうした課題に対して、NetNucleus Cloud Hubでは、監視・制御メッセージを中継するメッセージブローカを活用しWebSocket^{注1}で接続します。機器側から接続を確立してそれを維持することがポイントで、機器とブローカ間のダイレクト通信路を利用するため、ローカルネットワークに入る必要がなく、専用ゲートウェイや特別なFirewall設定なしで、既存ネットワーク環境のままリアルタイムアクセスが実現できます(図-1)。

(2) スケーラビリティ

遠隔監視・制御が大規模化し、スケールアウトするときはどうでしょうか。WebSocketなどのPush型通信はスケールアウトが困難です。データを収集するだけの一般的なPull型は既存のロードバランサ(負荷分散装置)で対応できますが、データの制御までを行う場合はロードバランサに負荷が集中してしまうケースがあります。

そこで、ロードバランサを使用せず、クライアントに接続先ブローカを教える接続調停サーバを採用しました。制御対象デバイスは、まず接続調停サーバに接続すべきメッセージブローカを照会し、接続調停サーバは適切なメッセージブローカの識別子を返します。エージェントソフトが指示されたメッセージブローカと接続し、WebSocketを維持します。その後、メッセージブローカの中継により制御端末はクラウドと直接やりとりすることになり、ロードバランサを使用した場合のロードバランサへ常にデータが流れる負荷を軽減できます。メモリ4GBのメッセージブローカ1台で12万台以上の機器収容も可能となることが実証確認されています(図-2)。

(3) セキュリティ

IoTを運用する上で、適切なアクセス権限を持ったユーザがセキュアにアクセスできることは極めて重要です。お客様によって、Webサイトは自分で作りたい、あるいは当社に開発を任せたいというケースもあるでしょうし、スマホアプリでの表示・閲覧や高度な解析サービスへの要望もあるかもしれません。お客様ごとに多様な形態のデータが存在し、また、アクセス権の所有者とデータの利用者が異なるケースも当然あるため、すべてのユーザが単にユーザのID、パスワードで認証すればよいというわけにはいきません。IDとパスワードのみの場合、連携・共有するアプリケーションがユーザのパスワードを知ることができるリスクもあり、ID・パスワードだけに依存しない認証の方法も不可欠となってきました。

NetNucleus Cloud Hubでは、ID・パスワードを用いた認証方式に加え、アクセストークンを用いた外部認証連携機能を提供しています。ログインはクラウドIoT基盤上で行い、アプ

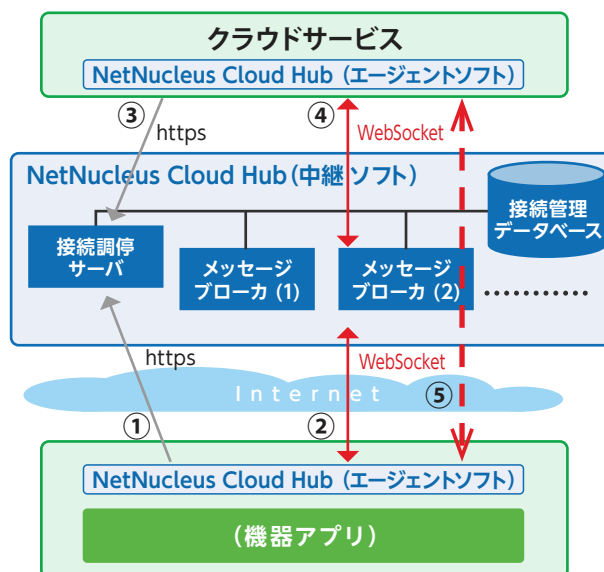


図-2 NetNucleus Cloud Hubの接続シーケンス

リケーションはユーザ認可の結果だけを受け取り、アクセストークン(クライアントがリソースオーナーに代わり認証済みリクエストを行うために使われる有効期間の短いトークン)をやりとりすることによって、サーバ上のデータにアクセスする仕組みです。アクセストークンを用いた認可方式に対応することで、多様な連携アプリとセキュアに連携することが可能となります。

パッケージの提供により 既存基盤への適用にも対応

このように、これまでスムーズなIoT化の妨げとなっていた数々の課題を解決できるソフトウェアパッケージとしてNetNucleus Cloud Hubの提供を2017年9月から開始しました。

クラウド側のソフトウェアはLinux/Windows対応の実行モジュールで、組込み機器側のソフトウェアは、Linux対応のC++ソースコードで提供します。AWSやMicrosoft Azure、オンプレミスなどにも適用可能で、既存の認証機能との連携も実現できます。また、このパッケージには、セキュリティパッチ版の提供、使い方に関するメールによる問い合わせ対応といったサポートも用意しています。

当社では本ソフトウェアパッケージを通じて、さまざまなプラットフォーム環境のお客様に対して、接続の容易性とリアルタイム性、セキュリティを確保しながらコストメリットのあるIoT運用実現に寄与していきたいと考えています。

(エンベデッドシステム事業部 山下 浩司)

注1) WebSocket : WebクライアントとWebサーバの間で双方向通信を実現する通信規格