Technical report

Secure IoT Gateway Architecture

プラントとクラウドの IoT プラットホームをつなぐ安全な IoT ゲートウェイアーキテクチャとは

産業向けに使用されている IoT ゲートウェイのアーキテクチャと、さらに安全性が強化されたアーキテクチャをご紹介します。

インダストリー 4.0 や産業用 IoT の登場により、プラントの制御システムをクラウドに接続することへの関心が高まってきています。クラウド上の IoT プラットホームを利用した遠隔監視は、プラントのデータを有効利用し生産性の向上に役立てられることが期待されています。機器からクラウドへ連携する方法の１つに、OPC UA を使用してデータを収集し、MQTT ゲートウェイを使用してクラウドに送信することがあげられます。セキュリティ面においても望ましい組み合わせになりますが、全てのユーザーのニーズを満たすとは限りません。まずは産業用の一般的な IoT ゲートウェイの構造を説明したうえでセキュリティを強化する方式を紹介します。

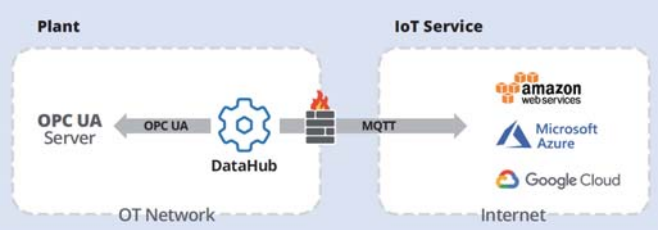
1．一般的な IoT ゲートウェイ

一般的な産業用 IoT ゲートウェイでは、プラント内とプラントからクラウドへの２つの通信を組み合わせます。

プラント内の通信には OPC UA が使用されています。OPC UA は、インダストリー 4.0 および産業用 IoT の安全な通信規格として推奨されていますが、これは OPC UA がアプリケーション層での認証と承認を含む多層セキュリティに加え、トランスポート層での証明書の使用による暗号化とデータの整合性を提供するためです。しかし、プラントからクラウドへ接続する場合は、プラントからクラウドへ接続できるようファイアウォールの外側からのポートを開く必要があるため、OPC UA は必ずしも安全とは限りません。

MQTT は、プラントからクラウドへの接続によく使用されています。Microsoft Azure、Google Cloud、Amazon IoT Core などのクラウドサービスでサポートされているため、IoT ゲートウェイに有用な通信規格です。MQTT を使用することでファイアウォールの外側からのポートを開かずに内側（プラント）から外側（クラウド）へのアウトバウンド接続を確立できます。これはプラントの制御システムの安全確保に不可欠な方式です。

Skkynet の DataHub IoT ゲートウェイソフトウエアは、OPC UA インターフェイスによりプラント内での安全な通信を提供し、MQTT によりプラントからクラウドへの安全な通信を提供できます。



※矢印は初期接続パスを示しています。接続確立後、双方向通信が可能となります。

すべての IoT ゲートウェイは、OPC UA のセキュリティ機能とデータ交換機能をサポートする必要があり、MQTT の安全な接続に加え、SSL 証明書ベースによってトランスポート層でのセキュリティもサポートする必要があります。この組み合わせにより、プラントのデバイスや機器からクラウドへの強固で安全な通信が期待できます。ただし、この接続方式にはひとつ欠点があり、OPC UA のデータをクラウドに送信する IoT ゲートウェイで「インターネットへの直接接続」が必要となります。企業のセキュリティポリシーでプラントからのインターネットへ直接接続が許可されていない場合は、直接接続をせずに安全にデータを送信するためのシステム要件が必要です。

2．DMZ とデイジーチェーン接続

さらに安全な通信を実現するために、多くの企業はプラントネットワークの内部と外部を分離した中間のネットワーク（以下「DMZ（非武装地帯）」）を設けています。そのほか、データを IT 側に送信し、データストリームの一部に接続し、クラウドに送信する方式も考えられます。実際、安全性の高いプラントはインターネットには直接接続されていないため、IT 部門または DMZ を介してデータを送信しています。どちらの場合も「デイジーチェーン」とも呼ばれるマルチホップが必要となります。

堅牢なデイジーチェーン接続では、各ホップは全ての受信データを確実に再送信すると同時に、チェーンに沿った任意の場所でネットワーク接続の障害をダウンストリームクライアントに通知する必要があります。しかしながら OPC UA も MQTT もこのユースケース用には設計されていません。

OPC UA は、クライアントがサーバーに直接接続され、サーバーが主要な情報源であることを前提としています。ところがデイジーチェーンでは、チェーンに沿ったホップがクライアントとサーバーの両方である必要があり、各ホップは元のサーバーのデータモデルと動作を再構築する必要があります。OPC UA は複雑であるため、このような再構築を行うことはできません。加えて、クライアントがサーバーに接続しなければならず、サーバーはクライアントが接続できるようリッスン状態にしておく必要があります。これを満たすには外側からのポートを開かなければならないため、回避したいシステム要件です。

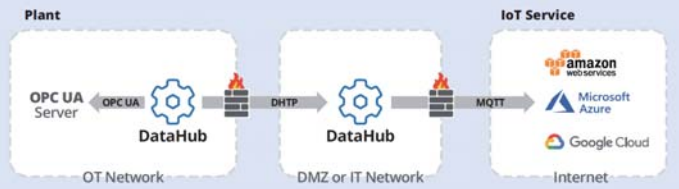
MQTT は特別に設計されたブローカとデイジーチェーン接続できますが、各ノードがチェーンの一部であることを認識し、個別に構成する必要があります。システム内のすべての MQTT クライアントは、他のすべてのデータソースとなる MQTT クライアントを認識しなければならず、各データ項目を接続元のステータスと関連付けるように構成する必要があります。この構成は、セキュリティを重要視するシステムにおいては、莫大なメンテナンスコストを必要とします。また、MQTT のサービス品質は、チェーン全体に伝播することができないため、このマルチホップではクライアントが最新の値を持っていることを保証できません。

※デイジーチェーン接続とは、一般的に複数の機器を数珠つなぎにつないでいく接続方法ですが、DataHub のデイジーチェーンとは、アプリケーションにおけるデータのデイジーチェーン接続を意味します。

3. DHTP で安全性が強化された IoT ゲートウェイ

産業用IoTに必要なのは、さらに強化された方式です。つまり、各ノードで完全なデータセットをミラーリングし、権限のあるクライアントとチェーン内のノードに対して、データへのアクセスを提供できる方式です。もちろん、これらは高いセキュリティを確保したうえで実現する必要があります。これにより、IT 部門はクラウドへ連携されているデータへ安全にアクセスすることができます。

この強化された方式は、各ノードにインストールされている DataHub などのミドルウェア製品を使用して実現できます。DataHub は、プラント上でファイアウォールの外部ポートを開かずに、プラント内ノードと DMZ または、IT 部門のサーバーの間でデータをトンネリングできます。そして DMZ または、IT 部門のサーバーにインストールされた２番目の DataHub は、MQTT サービスにデータを渡すことができます。



※矢印は初期接続パスを示しています。接続確立後、双方向通信が可能となります。

DataHub から DataHub への接続には、DataHub 転送プロトコル（以下「DHTP」）が使用されます。DHTP は、LAN、WAN、またはインターネットを介して TCP を使用してリアルタイムでデータを送受信します。プラントでの DataHub への OPC UA 接続はシングルホップです。さらに DataHub からクラウドへの MQTT 接続もシングルホップです。DHTP はデイジーチェーン接続を処理し、各ノードの完全なデータセットと接続ステータスをミラーリングします。DataHub を使用することで、アクセス権限のあるクライアントがアクセスできるだけでなく、チェーン内のノードにデータを渡し、データの一貫性も維持できます。DHTP のサービス品質は、通信帯域が不足して一部のイベントをドロップした場合であっても、チェーン内のすべてのクライアント、または中間ポイントが元のソースとデータの整合性を確保します。ネットワーク接続が失われた場合も、DataHub は関連するすべてのデータポイントのデータ品質を自動的に更新して、チェーン内のすべてのクライアントがデータ品質（ネットワーク接続の損失）をすぐに認識できます。

DHTP は DMZ、IT 部門、または別のインターネットノードを介して MQTT ゲートウェイ接続を安全に構成する実証された通信方式です。しかしながら、ほとんどの IoT ゲートウェイ製品はこの方式には適しておらず、一般的な IoT ゲートウェイアーキテクチャの OPC UA 通信、または MQTT 通信しか提供できていません。セキュリティに対し重要度が低いシステムでは問題ないかもしれませんが、産業用アプリケーションでは多くのシステム要件が必要となります。DMZ を使用してプラントを保護する必要がある場合、データをクラウドに渡す前に IT 部門に送信する場合、Skkynet の DataHub が堅牢で安全なソリューションを提供します。

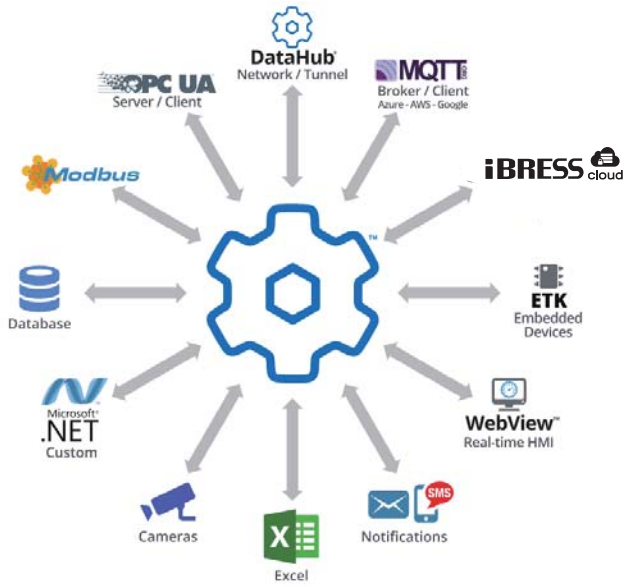
※本技術レポートは、Skkynet 社（カナダ）の Skkynet White Paper の『What Makes a Secure IoT Gateway Architecture?』の翻訳です。英語版と翻訳に相違がある場合、英語版の内容を優先するものとします 。
【英語版】What Makes a Secure IoT Gateway Architecture?
https://skkynet.com/secure-iot-gateway-architecture/

より詳しく知りたい方は裏面の問い合わせ先にて承ります。
常設展示ブースやセミナーも開催しておりますので、お気軽にお問い合わせください。

4. IoT ソリューションのご紹介

4-1. プラントとクラウドまでを容易に接続するミドルウェア DataHub

DataHub は、産業用通信 OPC（Classic や A&E、最新の UA）をはじめ、Modbus やデータベース、.NET アプリ連携、MQTT などクラウドサービスとのリアルタイムな双方向通信を確立する産業オートメーション向けのミドルウェアです。アラート通知や監視画面、冗長化などの多種多様な機能により産業データを最大限に活用いただけます。



DataHub の手軽さを体験してみてください。

DataHub 評価用ソフトを無料でダウンロード！

https://cogentdatahub.com/download/

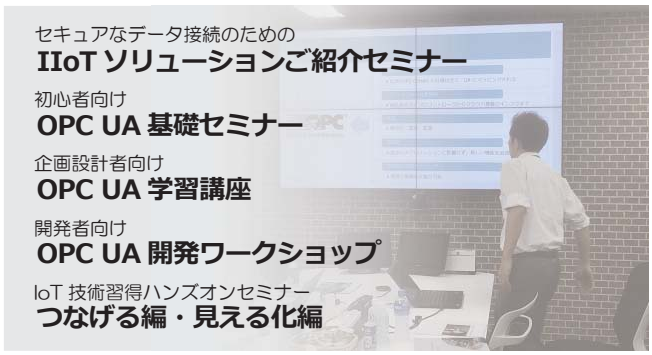
4-2. VPN を使わない安全な高速・双方向 データ通信サービス iBRESS Cloud

iBRESS Cloud は、お客様のパソコンにデータ接続用ミドルウェア『DataHub』を利用することで、アウトバウンド接続でプラントのデータをクラウドに送信できます。また DataHub でクラウドからデータを取り込むこともできます。

4-3. 来て！見て！試して！『IIoT Lab』

『IIoT Lab』は、2019 年 4 月に（株）ベルチャイルド 東京オフィス内に開設した「製造業向けの IoT」が体験できるユニークな施設です。センサやカメラ、PLC データを DataHub から iBRESS Cloud へ接続、データの可視化などを実際に機器を触りながら体験できます。

4-4. 充実のセミナー&ハンズオン

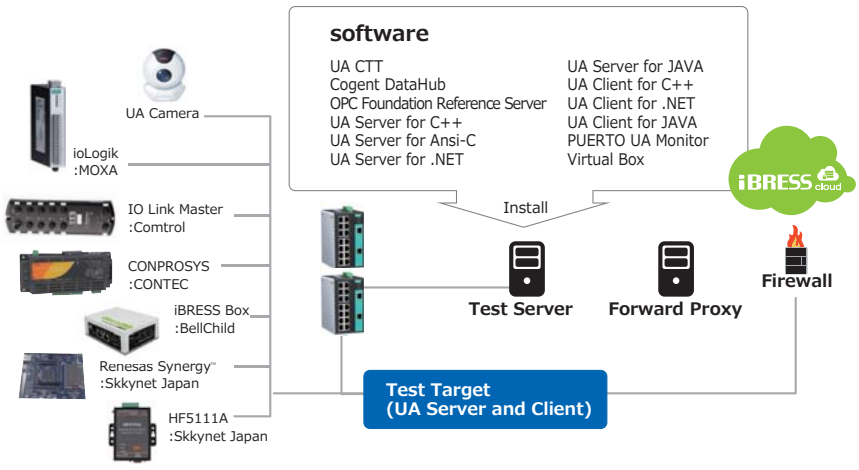


堅牢なシステム構築実現のため基本を DataHub や iBRESS Cloud を用いてデモや演習で学べる『IIoT ソリューションご紹介セミナー』、OPC UA の知識・動向が学べる『OPC UA 学習講座』、OPC UA 製品の開発に必要な知識の学習と接続から動作確認まで体験できる『OPC UA 開発ワークショップ』など多彩なセミナーを用意しています。

4-5. OPC UA 技術の評価ラボ

SKKYNET UA Lab.

インダストリー 4.0 の推奨ネットワークである OPC UA 機器の接続実験（Interoperability Test）、インターネット経由でのクラウド接続試験、ネットワーク負荷試験等を行うために国内外の多くのサーバ、クライアント機器、テストツールを用意しております。エンジニアリングコンサルティングも行っております。OPC UA の技術交流の場としてご利用ください。



Interoperability test devices

BellChild
株式会社ベルチャイルド
www.bell-c.co.jp

〒105-0013
東京都港区浜松町 2-5-5 PMO 浜松町 10F
TEL：03-5843-7502
FAX：03-5843-7503
E-mail：contact@ibress.com
http://www.ibress.com/

取扱店