IoTの普及に欠かせない、ネットワークの可視化とセキュリティ

FUJITSU JOURNAL / 2018年10月25日

生活を豊かにするIoT。一方で無視できないリスクも

あらゆる機器がインターネットに接続するIoTが、私たちの生活のさまざまなところに浸透してきています。例えば、自宅のエアコンがインターネットにつながり、外出先から操作できるようになったり、工場やビルに設備・機器の稼働状況を監視するセンサーが設置され、インターネットで遠隔制御・管理したりできるようにもなりました。農業にIoTを活用すれば、気温や湿度、土壌の温度などをセンサーで測定し、種まきに適した時期、肥料や水やりのタイミングなどを決めることも可能です。IoTの進展によって、私たちの暮らしや仕事がますます便利になっていくと期待されています。

一方で、IoTを活用したシステムが万が一止まってしまうと、工場の生産がストップしてしまったり、農場で育てている野菜が枯れてしまったりと、日常生活に支障がでてしまうことが懸念されます。

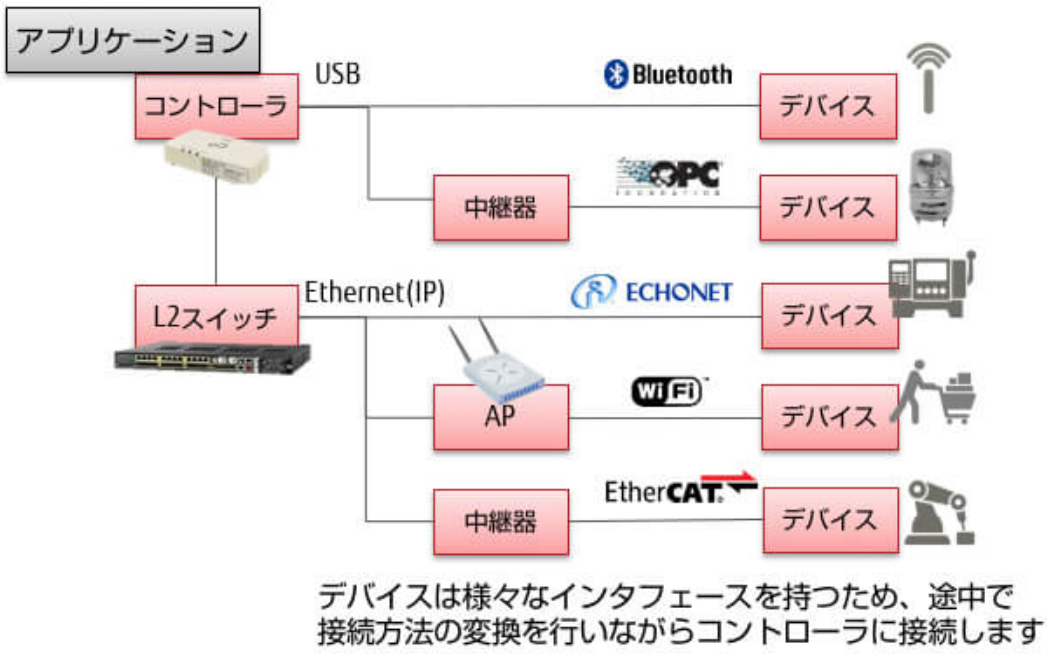
また、IoTデバイスはインターネットに接続しているため、外部からサイバー攻撃を受けるリスクもあります。実際、過去にはインターネットへの接続機能を備えた大量の監視カメラがマルウェアに感染し、サイバー攻撃に悪用された事件も起きました。日々の暮らしでも、「誰かにインターネット経由でエアコンの設定温度を勝手に変えられ、あやうく熱中症になるところだった」といったことも起こりえます。

このようなリスクを考慮しながら、IoTを安全かつ安心して利用するためには、デバイスやネットワークをしっかり管理して、問題が生じた際には迅速に対処できるようにしておく必要があります。

IoTデバイスの制御・管理が難しい理由とは

ところが、IoTデバイスの制御・管理には、じつは多くの課題があります。例えば、IoTデバイスはセンサーをはじめ、シンプルな構造で、パソコンやスマートフォンのように管理ツールやウイルス対策ソフトをインストールできるような機能を持ち合わせていないものがほとんどです。

また、工場やビルなどでは、さまざまな種類のIoTデバイスが設置されることが多く、IoTデバイスの接続はEthernetだけでなく、他の有線方式や無線方式など、複数の方式で接続することが多いです。さらに、家電、ガス、電気、ビル管理など、IoTデバイスを利用する分野ごとに、収集した情報をやりとりするための通信方式（プロトコル）が異なっているのが通常です。



IoTデバイスを接続するネットワークは複雑であり維持が難しい

最近では、インターネットの標準的なプロトコルであるTCP/IPに準拠している製品が増えてきましたが、工場などでは他の方式で通信するIoTデバイスが残っていることもあります。つまり、仕様

や形状、通信方式が異なる大量のIoTデバイスを、一括して制御・管理するのは簡単ではないのです。

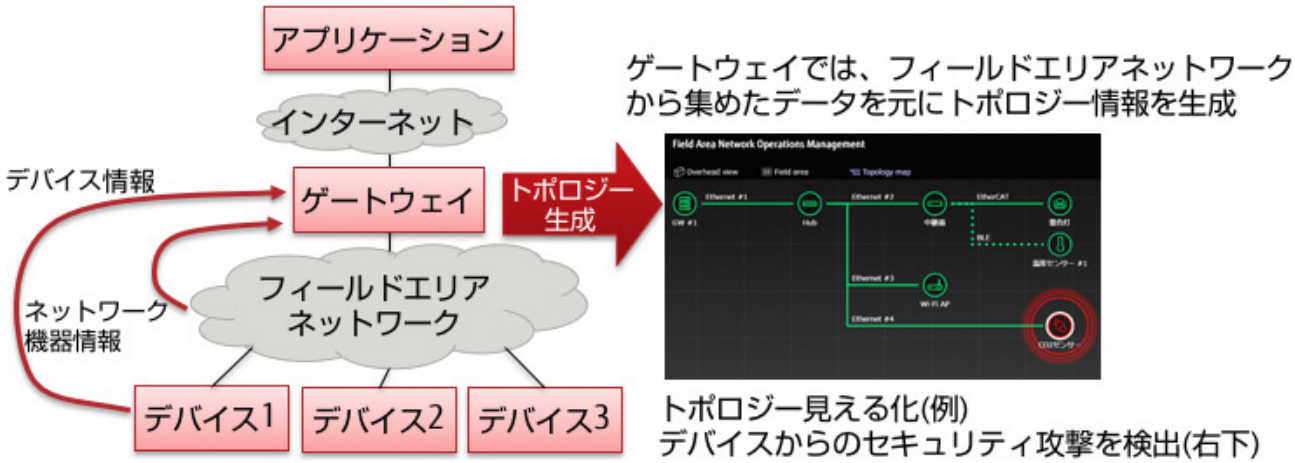
さらに、トラブルの原因が、IoTデバイスそのものの故障ではなく、ネットワーク障害で動作異常を起こすこともあります。例えば、工場内部の休憩室で使われた電子レンジとIoTデバイスを接続する無線ネットワークの周波数が一致したことで干渉が発生し、一部のネットワークの接続が切れてしまったということもありえるのです。

IoTデバイスがつながるネットワークを「見える化」する

このように接続方法、プロトコルがそれぞれ異なる、多種多様なIoTデバイスを管理し、安全かつ安心なIoTのネットワークを構築するにはどうすべきか。富士通は、IoTデバイスが接続されるネットワーク全体を「見える化」するという新たな発想でネットワーク制御技術を開発しました。

この技術では、IoTデバイスやその他の機器で構成されるネットワーク上に、異なるプロトコル同士での情報のやりとりを中継する「ゲートウェイ」を設置します。ゲートウェイはインターネットとIoTのネットワークを分離してパソコンと同様のセキュリティ対策が可能なため、外部からのデバイスへの攻撃を防ぐことができます。また、様々なプロトコルを解釈する機能も持っており、万が一、デバイスがマルウェアに感染した場合でも、「不審なふるまい」をするIoTデバイスの通信を発見することができます。

ゲートウェイでは、収集したデータからIoTデバイスやネットワーク機器など全体のトポロジー情報（デバイスやネットワーク機器のプロファイルおよび接続構成）を生成します。そうすると、どこで故障が発生したか、どのデバイスがサイバー攻撃をしているかなどの検知が可能になります。



トポロジー管理技術

IoTデバイスやネットワーク機器などネットワーク全体の接続構成を把握し、管理することで、例えばマルウェアに感染したIoTデバイスが、他のデバイスを攻撃しようとした場合、ゲートウェイが管理している正常な通信経路と、実際の通信経路を比較することで、不審な通信を発見できます。IoTデバイスごとの通信処理やデータ形式のパターンを管理しているので、通常とは異なる「不審なふるまい」をするIoTデバイスとして特定することができるのです。

今回開発したネットワーク制御技術では、TCP/IPだけでなく、工場などで利用されているさまざまなプロトコルにも対応しています。この方法を使えば、既存のIoTデバイスに手を加えることなく、IoTのネットワークを「見える化」できます。さらに、問題発生時にいち早く検知することで、サイバー攻撃への迅速な対処が可能になりますので、セキュリティ向上にもつながります。

IoTネットワークを制御し、企業の省エネ化、コスト削減を支援

ネットワーク制御技術の導入効果は、見える化による管理の効率化やセキュリティの向上だけではありません。各IoTデバイスの稼働状況を把握できれば、稼働率や故障率を知ることができます。それらの情報をもとに、「エネルギーロスの少ない機器の使い方」を検討するなど、省エネ、コスト削減に役立てることも可能です。

今後のIoTの普及を考えたとき、大切になるのは、安全かつ安心してIoTのネットワークを利用できるかどうかということ。多種多様なIoTデバイスの状況をしっかりと把握し、ネットワーク全体を「見える化」することが重要になります。富士通は、IoTの見える化を通して、さまざまな業種・業界における安全、安心なIoTの利用を支援します。

FUJITSU JOURNAL / 2018年10月25日