IoTビジネスプラットフォームにおけるネットワーク基盤

加藤　圭

IoT（Internet of Things）の世界的な普及が進み、今後、さまざまな事業領域に応じたIoTアプリケーションが開発されていくことが期待されている。また、AI技術の進展とあいまって、IoTのインフラから取得される大規模なデータを分析することで、工作機械などの故障予兆検知や、災害予測といったサービスも本格化していく。従って、これらのサービス提供のためには、インターネットを介した大容量データの送信が不可欠となり、既存ネットワークへのトラヒックが与える影響は非常に大きなものとなる。結果的に、予期せぬふくそうが発生し、サービスやアプリケーションが期待された動作ができないという事態が発生することも懸念されている。本稿では、これらの課題を解決し、お客様へのサービス品質の影響を最小限にするためのOKIのIoTビジネスプラットフォームのコンセプト、特長を紹介し、今後の取組みの方向性を示す。

背景

インターネットの爆発的な普及、個人、法人への定着、さらにはライフラインとしての重要性までも問われている現状で、ここ数年、IoTによる、モノをインターネットに接続し、モノからのデータを収集し、データ分析を行うサービス展開が進められようとしている。これは、今まで、人と人、あるいは、人とモノ（サーバーなど）を接続するためのインターネットであったものが、大量のモノとモノがインターネットで繋がるということになり、新たなパラダイムシフトが生じることを示す。つまり、モバイル網、固定網といったアクセス網の区別なく、インターネットのトラヒックパターンが、顕著にアップストリームの増大を招き、今までのネットワーク設計を見直さざるを得ない状況になることを示唆している。しかしながら、IoTの普及は、事業領域により普及の速度がまちまちであり、それらすべてのトラヒックを制御するネットワークインフラの提供者は、IoTの普及を予測して計画経済的に投資することが非常に難しい状況となってきている。IoT普及に向けて、IoT向けのインタフェースとして、LPWA（Low Power Wide Area）の導入が進められているが、コア網も含めた抜本的なインフラの改革は進んでいない。また、IoTも含めた将来の携帯網として、5Gの標準化も進められているが、サービスとしての提供は2020年以降といわれている。一方で、現在のIoTは、製造業、社会インフラ、運輸・物流などの現場に、センサーを設置し、それらのセンサーから得られる情報を、その場所（Field）から取得するためのセンサー網（FAN: Field Area Network）から、ゲートウェイを介して、3G/LTE,光ファイバー網経由でネットワークインフラを通り、IoTサービスを提供するプラットフォームが存在するデータセンターにデータを集めて分析などのサービスを提供するのが一般的である。その場合、ある事業領域でセンサーの普及が爆発的に進み、アップストリームデータが増大した場合、データセンターに集まるデータが非常に大きなものとなり、データセンターへの入り口の回線でのふくそうが想定される。また、日常的にこれらのサービスを提供する場合、データセンターで動作するアプリケーションの信頼性が非常に重要になる。運用上、高信頼ではないデータセンター上にIoTビジネスプラットフォームを設置した場合、激甚災害などへの対策が取れていないために、利用者の貴重なデータが失われる可能性もある。さらには、FAN上に配置したゲートウェイのセキュリティー対策をしていなかったために、データセンターへ侵入され、情報漏えいの問題も発生しうる。これらの課題を**図1**に示す。

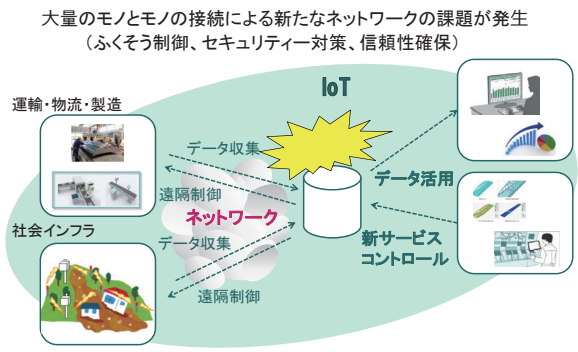

図1　IoTの普及に伴う課題

IoTビジネスプラットフォーム

現状、こういったインターネット環境を前提にすると、社会インフラなどのライフラインに直結するようなIoTアプリケーションの利用者は、専用線を用いる傾向にある。しかし、専用線は非常にビット単価が高く、また、インターネットではないため、IoTそのものがなかなか進展しない。一方で、コンシューマー向けの、間口の広いアプリケーションは、非常に安いSIMカードを用いて現状のインターネットを利用するが、セキュリティーへの課題や、通信品質に問題が発生する。そこで、OKIは、これらの課題を解決すべく、IoTビジネスプラットフォームを開発中である。これは、専用線になるべく近い高信頼なインフラを、極力低価格で提供可能とするプラットフォームである（**図2**）。

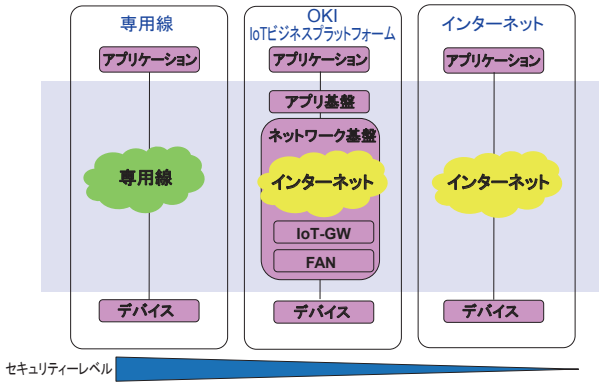

図２　IoT ビジネスプラットフォームの位置づけ

本IoTビジネスプラットフォームのネットワーク基盤は、以下の「つながる」「切れない」「低遅延」「セキュリティー」という４つのコンセプトで開発を進めている（**図3**）。これは、先述の課題である、「信頼性」を担保するための「切れない」技術、「ふくそう」に対処するための「低遅延」技術、情報漏えいなどの対策としての「セキュリティー」技術に加え、IoTのユーザーの利便性に寄与するための「つながる」技術で構成される。

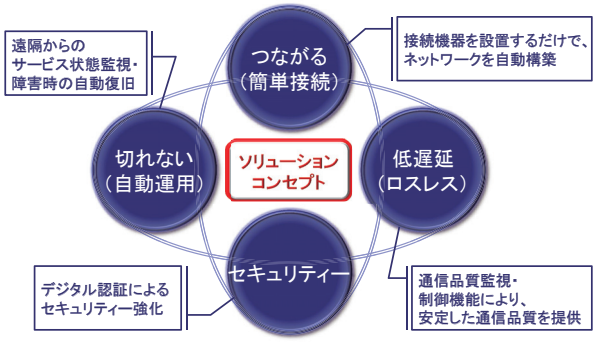

図３　ネットワーク基盤のコンセプト

＊1）Modbus は Modicon Inc.（AEG Schneider Automation International S.A.S.）の登録商標です。

(1)つながる

現在はIoTの黎明期であり、各事業領域で多くのセンサーを設置し、ネットワークに簡単につなげることが普及のために重要な要素となる。OKIは、IoTビジネスプラットフォームと簡単につながるソフトウェア（Zero　c onfiguration）を開発し、ゲートウェイに配備することで、ゲートウェイを立ち上げるだけで、自動的にクラウド上のIoTビジネスプラットフォームに接続し、データの収集、可視化、分析が行えることを可能とした。また、FANについては、OKIは920MHz帯マルチホップ製品を数多く展開しており、これを用いることで、さまざまな領域でのFAN設置が可能となる。また、Modbus＊1）RTUに準拠しているセンサーであれば、すべて接続可能となる。

(2)切れない

データセンター自体の信頼性に、IoTサービスの信頼性が極力影響を与えないために、IoTビジネスプラットフォームに高信頼ミドルウェア（HA-MW（High Availability Middleware）を独自開発した。本ミドルウェアは、電話交換機時代より開発、改良を加えてきたＯＫＩの独自開発製品であり、高信頼な音声通信を行うための呼処理システムの中で長期にわたり利用されていたもので、呼処理システムとしてはアベイラビリティ99.999%を担保することに寄与していた。これを用いることで、データセンターの影響を極力受けることなく、安定したIoTサービスを提供可能となる。

また、本IoTビジネスプラットフォームは常時、接続しているゲートウェイの状態を監視しており、問題発生時には、ゲートウェイの再起動などを遠隔で行うことで、ゲートウェイの信頼性向上を図っている.

(3)低遅延

センサーデータの増大に伴うデータセンターへの入り口回線のふくそう問題に対応するために、IoTビジネスプラットフォームに通信品質を監視する機能を設けている。これにより、ふくそうを監視し、ふくそう回避に必要な制御をゲートウェイに施すことが可能となる。たとえば、ふくそうの要因が、センサーデータ量が一時的に多くなっている場合、ゲートウェイでデータを圧縮してデータセンターへ送信したり、順序制御することにより、極力ふくそうを抑える仕組みが実現できる。

(4)セキュリティー

ゲートウェイがIoTサービスに接続する際に、セキュリティーの課題解決が重要となる。通常、ゲートウェイは、管理者がパスワードを入力し、そのパスワードをサーバーが認証する、いわゆるパスワード認証を行うが、工場や、屋外でパスワード認証を行う場合、成りすましによる情報漏えいは運用時の大きな問題として認識されている。そこで、OKIのIoTビジネスプラットフォームではデジタル認証方式を採用した。これは、ゲートウェイの出荷時にあらかじめデジタル証明書をゲートウェイに埋め込んでおき、現地での立ち上げ時、OMA-DMを用いて認証サーバーに本証明書で認証を自動的に行う方式である。これにより、利用者はパスワードを管理することなく、セキュアな運用が可能となる。また、今後、ゲートウェイへのDDoS攻撃など、可用性を脅かす課題が出てくるため、安全に運用できるセキュリティーインシデントモニタリングシステムを開発中である。

今後の方向性

上記コンセプトでIoTビジネスプラットフォームを開発、展開を進めていくが、今後、このプラットフォーム上で、さまざまな事業領域でのアプリケーション開発が加速していく。そこで、OKIはこのIoTビジネスプラットフォーム内に、多くの事業機会に水平的に利用可能なアプリケーションパッケージを開発推進する予定である（図4）。

図４　IoT ビジネスプラットフォームのレイヤー構造

これにより、複数の事業領域でも、共通機能が利用可能となり、導入コスト削減に寄与する。本アプリケーションパッケージは、柔軟な構成を持つため、他の分析エンジンなどが他のクラウドにある場合、容易に連携が可能である。また、さまざまな領域でのデータ収集を進める中で、データの蓄積により、多くの知見を得ることが可能となる。これらの複数の事業領域でのサービス展開を可能とするために、IoTビジネスプラットフォームはマルチテナント管理を容易に行う仕組みをすでに実装している。これにより、事業領域ごとに情報は閉じた管理をする中で、運用管理など、機密情報に触れずに各事業領域のテナント管理が可能となり、水平展開を容易にしている。

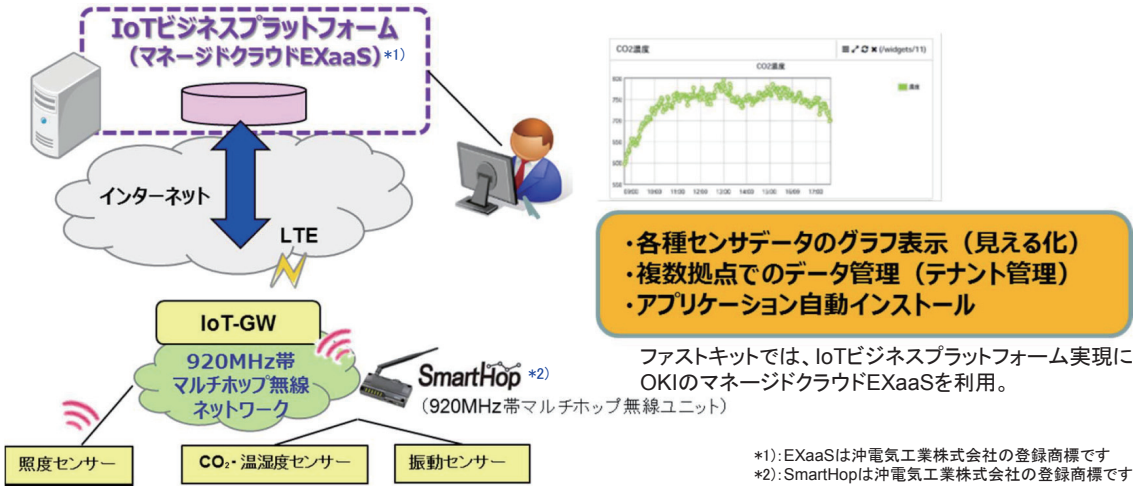

図５　IoT ファストキット

また、今後のIoTの普及を促進する目的として、お客様に対して本IoTビジネスプラットフォームを簡単に利用するためのスタートアップキット「IoTファストキット」を現在展開中である（**図5**）。これは、代表的なセンサー（温湿度センサー、照度センサー、振動センサー、CO_2センサーなど）を920MHz帯マルチホップ無線ユニットを介して、ゲートウェイまでをパッケージとし、お客様が組み立て、電源を入れるだけで簡単に可視化が可能となるキットである。これを導入していただき、実際にセンサーデータを取得し、課題を抽出することで、適切なアプリケーションをプラットフォーム内で開発でき、お客様にマッチしたアプリケーションを、高品質なIoT環境で安価に提供することが可能となる。

まとめ

現在のIoTの普及がおよぼすネットワークインフラへの影響を想定し、今後のIoT普及を後押しし、かつ、IoT普及に伴う、さまざまなネットワークインフラへの課題を解決するIoTビジネスプラットフォームを紹介した。今後、IoTビジネスプラットフォーム内に新たにアプリケーションパッケージを構築し、さまざまな事業領域への展開を進める。 ◆◆

●筆者紹介

加藤圭：Kei Kato. 情報通信事業本部 新規事業開発室

TIPS【基本用語解説】

LPWA（Low Power Wide Area）
IoT等に適用するための通信規格として、デファクトおよび標準化の両面で開発が進められている。センサーから得られるデータは一般的には非常に小さなパケットであり、かつ、それらを長距離で基地局へ送信する必要がある。また、屋外等で使われることも考慮すると、省電力が求められる。これらを満たす通信規格をLPWAと言う。

LTE（Long Term Evolution）
移動網の標準化団体である 3GPP（Third Generation Partnership Project）によって標準化され、2010 年よりサービスが開始されている。LTE で音声を流す規格も 3GPP にて標準化されており、VoLTE（Voice over LTE）と呼ばれ、2012 年よりサービスが開始されている。

アップストリーム
ネットワークを介した通信では、通常、人あるいはモノからサーバーの方向へ流れる通信をアップストリームという。反対に、人あるいはモノからサーバーへの方向へ流れる通信をダウンストリームという。

OMA-DM
Open Mobile Alliance Device Managementの略。携帯端末等のアプリケーションの標準化団体である、Open Mobile Allianceが標準化したデバイス管理機能。サービス開始前の端末にサーバーから設定するためのプロトコル等が規定されている。

Zero configuration
端末や通信機器を、ユーザーが設定することなく、電源を投入するだけで接続可能とする機能のこと。当初はインターネットの標準化団体であるIETF（Internet Engineering Task Force）が通信機器の標準化を行う際にこの用語が用いられていた。

DDoS攻撃
Distributed Denial of Service の略。ネットワーク上で、通信設備や端末、サーバーに対して、悪意を持ったユーザーが、大量のトラヒックを流して、設備を利用不能にしてしまうことをDenial of Serviceという。これを、複数の不特定多数の方向から一斉に行うことで、集中的にかつ誰が攻撃したかわからない状態で攻撃を行うことをDDoS攻撃という。

セキュリティーインシデントモニタリングシステム
DDoS攻撃のように、設備等に対して影響を及ぼしうる状況をセキュリティーインシデントと呼ぶ。これを監視するためのシステムをセキュリティーインシデントモニタリングシステムと呼ぶ。

920MHz帯マルチホップ無線ユニット
電波到達性が高く、障害物があっても回り込んで届く920MHz帯無線を採用し、OKI独自のマルチホップ無線技術を搭載した商品。複数の無線装置を経由して、バケツリレーのようにデータを伝送する通信方式。親機から直接電波が届かなくても近隣の子機を経由してネットワークに接続できるため、広いエリアの無線ネットワークを低コストで構築できる。また、電波状態の良い経路を自動的に選択して通信するため、一時的な電波障害に強く信頼性に優れている。