特集論文

IoTシステム対応三菱通信ゲートウェイ

大野聖信* 山口晃由**
横里純一*
富澤俊明*

Mitsubishi Communication Gateway for IoT System

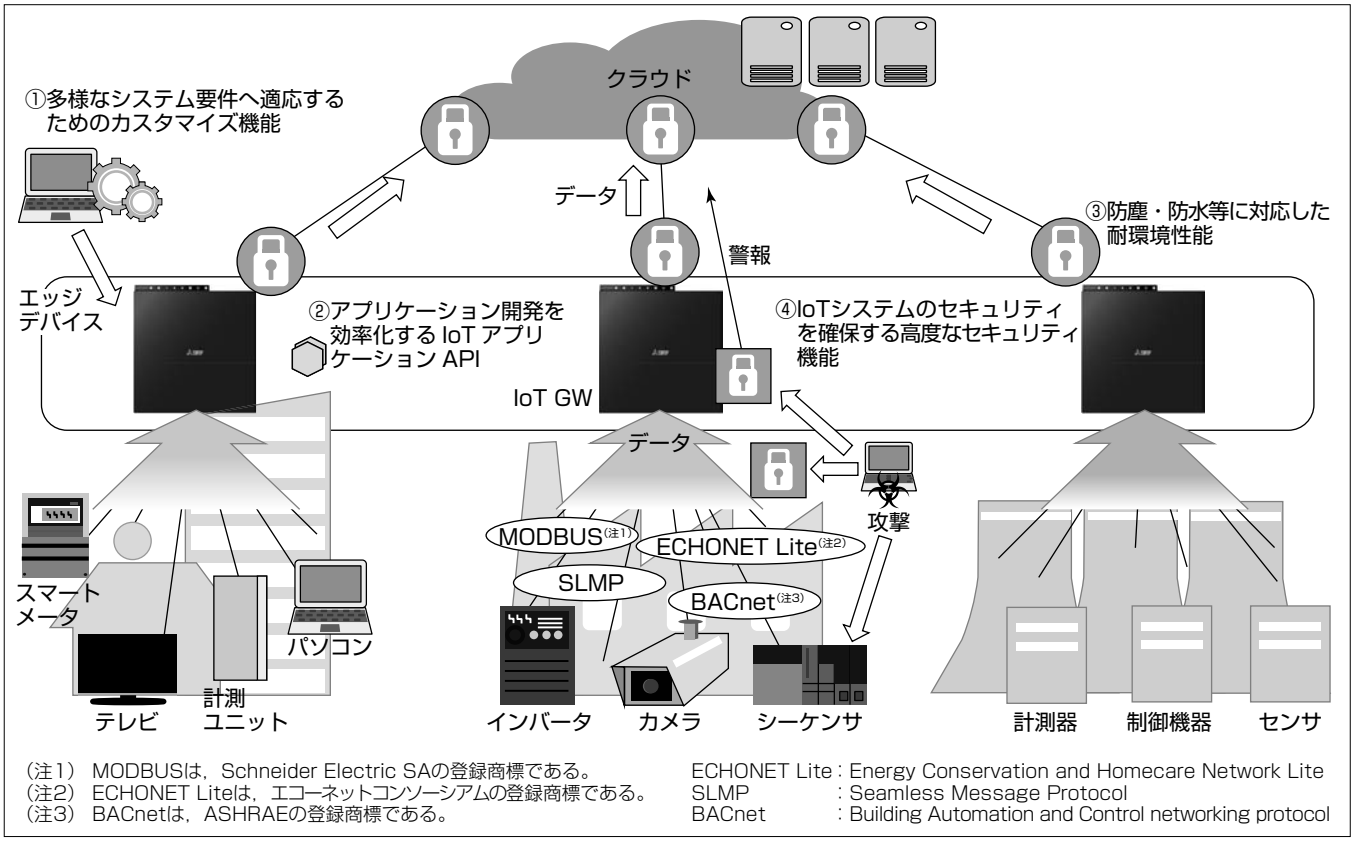
Toshinobu Ono, Junichi Yokosato, Toshiaki Tomisawa, Teruyoshi Yamaguchi

要 旨

近年，カメラやセンサ等から収集したデータを，故障解析や作業の効率化，災害予測などに活用するIoT(Internet of Things)システムの適用事例が増えている。IoTシステムでは，大量のデータを処理するクラウドの負荷を軽減するため，機器とクラウドの間で，クラウドへ送信するデータの選別・集約・加工等の一次処理を行うエッジデバイスが重要な役割を果たす。

一次処理の内容や，一次処理で使われる機能，エッジデバイスの設置環境は，いずれもシステム要件によって多様である。このため，エッジデバイスには利用するクラウド，センサ，通信プロトコルなどに応じて必要な機能を柔軟に選択できること，選択した機能を利用するアプリケーションを容易に開発できること，設置環境を選ばないことが要求される。また，サイバー攻撃によって，製鉄所の溶鉱炉が制御不能になるなどの被害が報告されており，IoTシステムのセキュリティ確保も重要な課題である。

これら市場の要求に対応するため，三菱電機ではエッジデバイスとしてIoTシステム対応三菱通信ゲートウェイ(IoT GW)を開発した。この装置は，多様なシステム要件に適応するためのカスタマイズ機能，アプリケーション開発を効率化するIoTアプリケーション対応API(Application Programming Interface)，防塵(ぼうじん)・防水等に対応した耐環境性能，IoTシステムのセキュリティを確保する高度なセキュリティ機能を備えている。今後，これらの特長を活用して社会インフラ，交通，産業，くらしの様々な分野で新たな付加価値を創出し，快適・安心な社会を実現していく。



(注1) MODBUSは，Schneider Electric SAの登録商標である。
(注2) ECHONET Liteは，エコーネットコンソーシアムの登録商標である。
(注3) BACnetは，ASHRAEの登録商標である。

ECHONET Lite : Energy Conservation and Homecare Network Lite
SLMP : Seamless Message Protocol
BACnet : Building Automation and Control networking protocol

IoT GWを用いたシステム構成

IoT GWは，有線／無線LANやRS485，USB，LTE(Long Term Evolution)等の多様なインタフェースを介してデバイスと接続することが可能である。さらに，カスタマイズ機能，IoTアプリケーション対応API，防塵・防水等の耐環境性能，高度なセキュリティ機能を備える。

*コミュニケーション・ネットワーク製作所 **情報技術総合研究所

1. まえがき

近年，カメラやセンサ等から収集したデータを，故障解析や作業の効率化，災害予測などに活用するIoTシステムの適用事例が増えている。IoTシステムでは，大量のデータを処理するクラウドの負荷を軽減するため，機器とクラウドの間で，クラウドへ送信するデータの選別・集約・加工等の一次処理を行うエッジデバイスが重要な役割を果たす。

一次処理の内容や，一次処理で使われる機能，エッジデバイスの設置環境は，いずれもシステム要件によって多様である。このため，エッジデバイスには利用するクラウド，センサ，通信プロトコルなどに応じて必要な機能を柔軟に選択できること，選択した機能を利用するアプリケーションを容易に開発できること，設置環境を選ばないことが要求される。また，サイバー攻撃によって，製鉄所の溶鉱炉が制御不能になるなどの被害が報告されており，IoTシステムのセキュリティ確保も重要な課題である。

これら市場の要求に対応するため，当社はエッジデバイスとしてIoTシステム対応三菱通信ゲートウェイ(IoT GW)を開発した。

本稿では，最初にエッジデバイスの役割と要求条件を述べ，次にカスタマイズ機能，IoTアプリケーション対応API，耐環境性能，高度なセキュリティ機能について述べる。

2. IoTシステムでのエッジデバイス

2.1 エッジデバイスの役割

IoTシステムでは，カメラやセンサ等の機器からデータを収集し，クラウドに設置されたサーバでデータを処理し，必要な制御や判断を行う。しかし，機器から直接クラウドへ全てのデータを送ると，サーバの処理負荷が高くなる。また，リアルタイム性が要求されるシステムでは，機器とクラウド間の通信遅延が問題となる。さらに，データの盗聴・改竄(かいざん)のリスクも高まる。そこで，機器とクラウドの間で，データの選別・集約・加工等の一次処理を行い，暗号化してクラウドへ送信する中継装置が使用される。この中継装置をエッジデバイスという。エッジデバイスの設置場所と役割を**図1**に示す。

エッジデバイスの役割は次の3つである。

①配下機器から収集したデータを一次処理してクラウドへ送信する。

②配下機器の通信プロトコルからクラウドの通信プロトコルへ変換する。

③クラウドへ送信するデータを暗号化してエッジデバイスとサーバ間のセキュアな通信を実現する。

2.2 エッジデバイスへの要求条件

(1) 柔軟なカスタマイズ機能

多様なシステム要件に対応するためには，エッジデバイスでは使用する機能の構成や各種設定の初期値，項目別のカスタマイズ権限等を細かく設定できる必要がある。一方で，過剰なカスタマイズ項目は設定を複雑化させてミスを誘発してしまうため，カスタマイズ項目を必要最小限に限定できることが望ましい。これらのニーズに合致した柔軟なカスタマイズ機能が求められる。

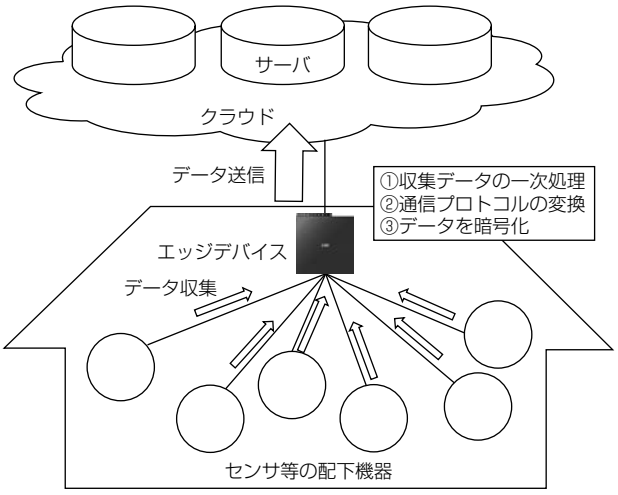


図1．エッジデバイスの設置場所と役割

(2) アプリケーションを容易に開発できる仕組み

エッジデバイスで一次処理を実行するためには，IoTシステムごとに，配下機器のハードウェア，通信プロトコル，システム要件に合わせてアプリケーションソフトウェアを開発する必要がある。このため，多岐にわたるハードウェア，通信プロトコルへの対応を容易とし，短期間・低コストでアプリケーションを開発できる仕組みの提供が重要である。

(3) 耐環境性能

エッジデバイスは，一般家庭や企業のオフィスなど空調管理された環境だけではなく，工場や機械室などの高・低温環境，塵(ちり)や埃(ほこり)が発生しやすい環境，工場水を扱うような環境での利用も想定される。このため，エッジデバイスには広い動作温度範囲と防塵・防水構造が求められる。

電源はAC100Vだけでなく，DC電源，PoE(Power over Ethernet)給電が使われるケースも多く，多種な電源タイプへの対応が求められる。

(4) セキュリティ確保

工場やプラントでの産業システムでは，IoTシステム導入によって外部ネットワークと接続されるケースが増えるため，ITシステムと同様にサイバー攻撃の脅威に晒(さら)されるリスクが高くなる。しかし，一方で従来のITシステム用のセキュリティ技術では，大量の不審パターンのモニタ及び解析が必要であり，高速な応答が困難である。このため，一定のリアルタイム性が必要なIoTシステムでは，高速応答を実現する新たなセキュリティ技術が求められている。

3. IoT GW

開発したIoT GWは，カスタマイズ機能，アプリケーション開発を効率化するIoTアプリケーション対応API，防塵・防水等に対応した耐環境性能，高度なセキュリティ機能を備え，**2. 2節**で述べた要求条件に応える。

3. 1 カスタマイズ機能

エッジデバイスでは，多様なシステム要件に対応するために機能の構成や初期値，カスタマイズ権限等を細かく設定できる必要がある。IoT GWでは，カスタマイズ機能を実装し，次のようなカスタマイズを可能とした。

⑴ 機能構成定義

図2に示すように，システム構築に必要な機能のみを有効化し，機能構成を定義することができる。有効化しなかった機能は，管理画面には表示されないため，エンドユーザーによる不用意な変更を防ぐことができる。

⑵ 初期値変更

システム要件に対応して各種設定の初期値を変更可能とした。また，工場出荷時の状態だけでなく，カスタマイズ後の状態に戻すことも可能な二段階の初期化機能を持っている。

⑶ カスタマイズ権限設定

エンドユーザーごとに項目別のカスタマイズ権限を設定可能とした。また，HTTP等を使用したリモートからのカスタマイズ機能によって，システム構築後の設定変更にも柔軟に対応できる。

3. 2 IoTアプリケーション対応API

IoTアプリケーションの開発を容易にするため，IoT GWでは，Java仮想マシン(Java VM(注4))を搭載した。アプリケーションはJavaVM上で動作するため，異なるハードウェアやOS上で実行できる。これによって，IoT GWのハードウェア構成を意識することなく，Java標準開発ツールを利用することが可能となる。

IoTシステムで使われる各種の通信プロトコルはクラウドや配下機器によって異なるため，システムに合わせたプロトコルの実装が必要となる。そこで，各種の通信プロトコル，ゲートウェイ制御機能をあらかじめモジュール化し，APIとして提供する。これらを使用することで，容易にIoTアプリケーションを開発することができる。**図3**にIoT アプリケーション対応APIの例を示す。

⑴ ゲートウェイ制御API

ゲートウェイ装置内の機能(LED制御，USB制御，ネットワークインタフェース制御等)を使用するためのAPIを提供する。

⑵ 通信プロトコルAPI

クラウドとの通信プロトコルであるHTTP(S)，MQTT，OPC UA[1]等と，配下機器の通信プロトコルであるMODBUS，ECHONET Lite[2]，SLMP，BACnet等に対応したAPIを提供する。

(注4) Javaは，Oracle Corp.の登録商標である。

3. 3 耐環境性能

IoT GWの概略仕様を**表1**に示す。多様な設置環境に対応するための耐環境性能を備えている。

⑴ AC／DC／PoEの各電源入力への対応

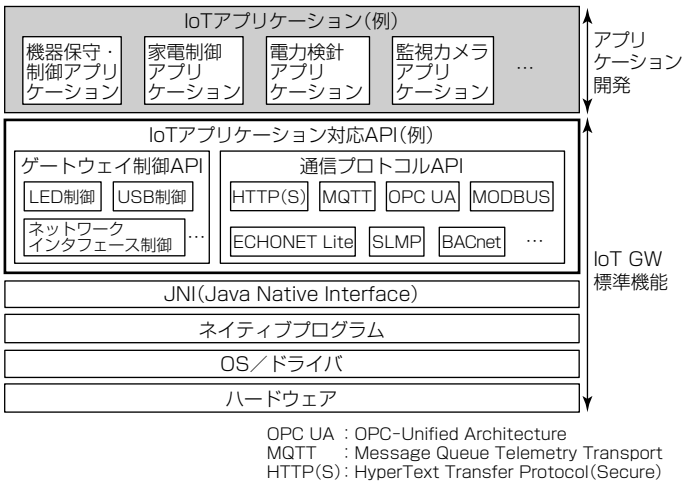


図3．IoTアプリケーション対応APIの例

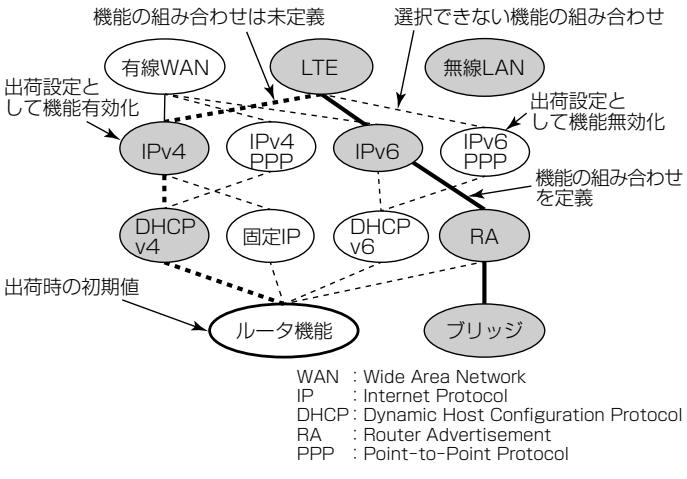


図2．カスタマイズ機能の例

表1．IoT GWの概略仕様

項目		諸元
外部インタフェース	WAN	1000BASE-T，1ポート
	LAN	1000BASE-T，4ポート
	USB	USB2.0，2ポート
	無線	LTE／無線LAN
	シリアル通信	RS-485，1ポート
	SDカード	microSDスロット，1ポート
構造諸元	外形寸法	67.5(W)×230(D)×230(H)(mm)
環境諸元	動作周囲温度	−10〜55℃
	動作周囲湿度	10〜90%，結露なし
	防塵・防水	IP53
電源諸元	電圧(ACアダプタ)	AC100〜240V，50／60Hz
	電圧(DC端子台)	DC24V
	PoE(受電)	IEEE802.3af クラス0対応
	消費電力	22W以下

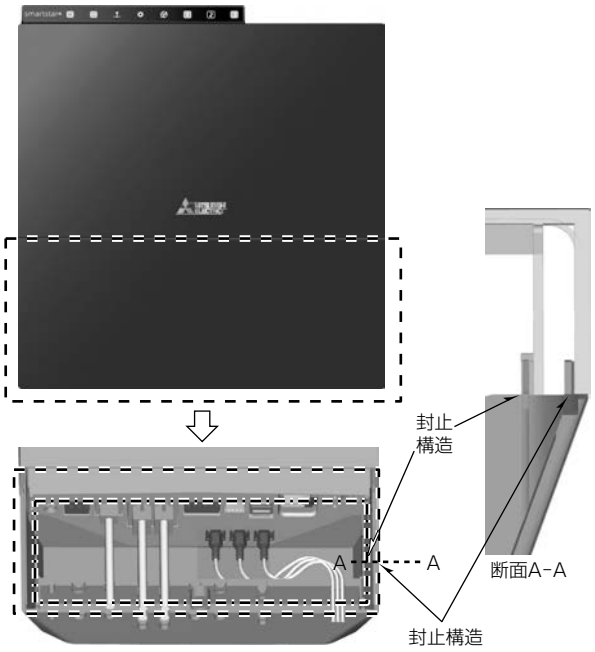


図４．IoT GWと封止構造

⑵　空調非設置環境での使用を想定した広範な動作温度範囲の実現(動作周囲温度-10～55℃)

⑶　保護等級IP53(注5)の防塵・防水性能の実現

筐体のインタフェース部の封止構造を二重にすることで，多様なインタフェースをサポートしつつ，小型筐体(きょうたい)に最小限の防護構造で防塵・防水性能を実現した(**図４**)。

(注５)　防塵等級IP5X，防水等級IPX3

3.4　セキュリティ機能

⑴　攻撃検知機能

産業システムに代表される多くのIoTシステムでは，従来のIT 系システムに比べて，装置やアプリケーションを変更する機会が少なく，送受信先や送信データなどの通信パターンが固定的である場合が多い。この特徴を利用して，IoT GWにホワイトリストを用いた攻撃検知機能(3)(4)を搭載した。

攻撃検知機能の動作を**図５**に示す。ホワイトリストは，従来のルータでも照合しているIPアドレス，ポート番号等に加えて，正常な通信属性(通信周期，コマンド種別，データの受信順序等)がリスト化されたものである。攻撃検知機能は，制御ネットワークを流れる通信データをキャプチャしてホワイトリストと照合する(**図５**①)。監視制御装置がマルウェアに感染し，機器制御コントローラやサーバが正常時とは異なるパターンの通信を行った場合(**図５**②)，攻撃検知機能がこれを検知し，外部ネットワークを通じてSOC (Security Operation Center)等のセキュリティ監視システムに報知する(**図５**③)。

このように，攻撃検知機能は，システムが不安定になる前にサイバー攻撃を検知し，報知することができる。

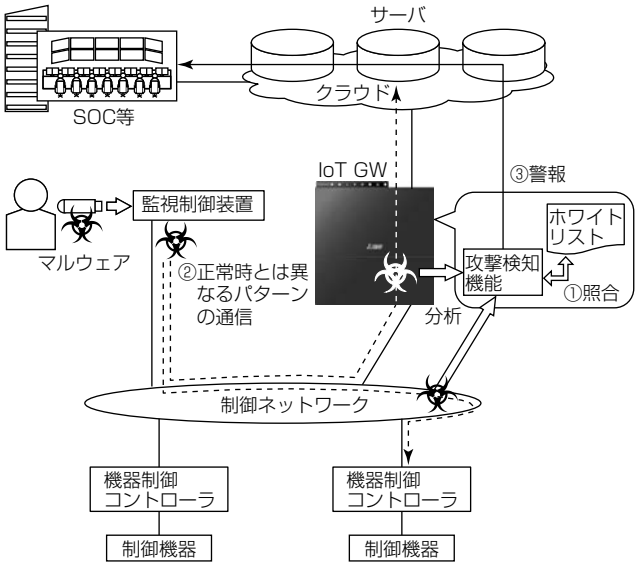


図５．IoT GWに搭載する攻撃検知機能

⑵　EDSA認証FSAレベル１相当機能

IoT GWでは，産業用制御機器のセキュリティ認証制度であるEDSA(Embedded Device Security Assurance)認証の機能要件として定義されるFSA(Functional Security Assessment)レベル１相当の機能を実装した。また，SDSA(Software Development Security Assessment)レベル１相当のセキュアなソフトウェア開発プロセスに従って開発し，通信ロバストネス試験を実施している。これによって，IoT GW自身のセキュリティを確保した。

4. む　す　び

様々なIoTシステムに適用可能なIoT GWについて述べた。IoT GWでは，多様なシステム要件へ適応するためのカスタマイズ機能，アプリケーション開発を効率化するIoTアプリケーション対応API，防塵・防水等に対応した耐環境性能，IoTシステムのセキュリティを確保する高度なセキュリティ機能を備えている。

今後もIoT GWの機能充実化を図り，多くのシステム事業分野でIoTによる新たな付加価値を創出し，快適・安心な社会の実現に貢献していく。

参　考　文　献

⑴　OPC Foundation：OPC Unified Architecture(IEC 62541)

⑵　エコーネットコンソーシアム
http://www.echonet.gr.jp/

⑶　山口晃由，ほか：産業制御システムにおける侵入検知手法の調査と検討，SCIS2015，2A4-3 (2015)

⑷　中井綱人，ほか：プラント制御システム向けホワイトリスト型攻撃検知機能の設計，SCIS2016，2B2-4 (2016)