エッジコンピューティングを実現する社会インフラ・産業分野向け IoTゲートウェイ装置

IoT Gateway Device Realizing Edge Computing for Social Infrastructure and Industrial Fields

中嶋　宏　　松本　賢一郎
■NAKAJIMA Hiroshi　■MATSUMOTO Kenichiro

社会インフラ・産業分野向けのIoT（Internet of Things）であるインダストリアルIoTでは，大量のデータを集めて分析するため，監視制御対象の機器が置かれている現場（エッジ）側とクラウドシステム側の間で最適な処理分担を図り，エッジ側でもデータの処理や分析を行うエッジコンピューティングが重要になると考えられる。エッジコンピューティングによって，現場の状況や機器の微細な変化をIoTゲートウェイ装置で迅速かつ的確に把握できるようになり，更にインテリジェントな処理を組み込んだエッジリッチコンピューティングによって，新たな価値を創造することも可能になる。

東芝デジタルソリューションズ（株）は，このようなインダストリアルIoTに求められるエッジコンピューティングを実現するIoTゲートウェイ装置を開発した。様々な監視対象機器，発信されるデータ，及び必要な分析処理をソフトウェア定義によって自在に構成できる仕組みを備えることで，柔軟なエッジコンピューティングを実現し，かつ段階的に進化させられるようにした。また，東芝グループ内の技術を結集し，インダストリアルIoTに求められる，耐環境性，長期信頼性，及びセキュリティー脅威に対する堅牢（けんろう）性を備えたハードウェアを実現した。

In order to accumulate and analyze large volumes of Internet of Things (IoT) device data in the social infrastructure and industrial fields, it is important to achieve a balance between cloud computing resources and edge computing resources. Edge computing enables users to promptly and accurately grasp the actual situation of equipment and fluctuations in its performance using IoT gateway devices. This, in turn, becomes the basis of the more intelligent rich edge computing to create new business value.

Toshiba Digital Solutions Corporation has developed a novel IoT gateway device for edge computing in these fields. This device has an architecture that allows flexible edge computing and ongoing operational improvements by providing software platforms that can configure various devices, data, and data processing operations in supervisory and control systems. Furthermore, we have realized environmentally durable, highly reliable, and securely robust hardware for this IoT gateway device using the comprehensive technologies in these fields accumulated by the Toshiba Group.

1　まえがき

インダストリアルIoTでは，大量のデータを集めて分析するため，エッジ側とクラウドシステム側の間で処理の最適分担を図り，エッジ側においても分析処理を行うエッジコンピューティングが重要になると考えられる。このエッジコンピューティングによって，現場の状況や機器の微細な変化をIoTゲートウェイ装置で迅速かつ的確に把握できるようになり，クラウドシステム側とのデータ通信量やクラウドシステム側でのデータ処理の負荷を軽減できる。更にメディア処理やAIなどのインテリジェントな処理を組み込むことで，新たな価値を創造することが期待されている。

エッジ側は，稼働中の設備も含めて多様な機器を接続できるマルチデバイス対応であるとともに，最適なサービスを提供する様々なクラウド基盤と接続できるマルチクラウド対応であることが求められる。更に，過酷な環境への対応，システムの長期安定稼働，及び強固なセキュリティーも実現する必要がある。

今回，東芝デジタルソリューションズ（株）は，このようなエッジコンピューティングを実現するインダストリアルIoTに向けたゲートウェイ装置のソフトウェアとハードウェアを開発した。ソフトウェア定義によってマルチデバイス及びマルチクラウドに対応することで，柔軟なエッジコンピューティングを実現し，現場に適合しやすい構成が取れるようにした。ハードウェアは，東芝グループの産業用コンピューターやPC（パソコン）での技術蓄積を生かし，耐環境性，長期安定稼働，及び高いセキュリティーを実現した。

ここでは，インダストリアルIoTを対象としたエッジコンピューティングに求められる要件や，それらに対応したIoTゲートウェイ装置のソフトウェア定義を基軸としたエッジアーキテクチャー，耐環境性をはじめとしたハードウェアなどについて述べる。また，この製品を適用したシステム事例についても述べる。

2　インダストリアルIoTを対象としたエッジコンピューティングに求められる要件

インダストリアルIoTが対象とするのは，工場の生産ラインや社会インフラシステムを構成する機器であり，異常の発生や

予兆などの元となるような状態の変化を，ミリ秒オーダーのデジタルデータとして迅速かつ的確に検知できなければならない。また，システムの稼働状態を詳細に把握するためには，大量のセンシングデータが必要になる。

大規模なストレージと高い処理能力を柔軟に構成できるクラウドコンピューティングは，IoTのビッグデータ分析に不可欠である。しかし，装置が設置された現場からクラウドシステムまでのデータパスは長く，クラウドコンピューティングがミリ秒オーダーで応答することは現実的ではない。また，大量のセンシングデータを多数の装置から同時に受け取ることは，クラウドコンピューティングのコスト増大を招く。

したがって，現場の装置からクラウドシステムまでのコンピューティングを階層的に捉え，それぞれの処理能力と，センシングデータに対する処理頻度の要求バランスを考慮して，階層間で処理を最適分担することが求められる。東芝IoTアーキテクチャーSPINEX™はこの考え方に基づいており，(1)PLC (Programmable Logic Controller) などがセンシングデータを直接取得するデバイス層，(2)デバイス群をネットワーク化するとともに，センシングデータの一次処理や，イベント分析，バッファリングなどを行うエッジ層，(3)迅速性やデータ保護の観点からローカルサイトでデータ分析を行うフォグ層，及び(4)全サイトのデータを集約して機器の稼働状態の見える化や分析を行うクラウド層の4階層で構成されている（**図1**）。(2)のエッジコンピューティングが，インダストリアルIoTに求められる迅速性の実現と，クラウドシステムと協調したビッグデータ処理を可能にする役目を担っている。

エッジ層は，製造機械や，ロボット，PLCなど多様な装置からセンシングデータの収集，蓄積，及びイベント検知を行い，更にデータ解析などの処理も行う。エッジ層でこれらの多様な装置を接続するには，様々なプロトコルやデータ構造に柔軟に対応できなければならない。生産ラインの稼働を継続しながら，既設あるいは新設の装置を徐々にエッジ層のネットワークに取り込み，更に将来にわたってデータの分析結果を基にエッジ側での処理を機能的に進化させ続けられる，適応性や拡張性も必要である。

クラウド層は，目的に適した各社のクラウドサービスを複数選択して，様々なクラウドサービスを容易にシステムに組み込めるものでなければならない。

ハードウェアに目を向けると，社会インフラ・産業分野で使用される装置は，例えばエレベーターや，大型発電機，工作機械，ロボット，車両，動力装置などであり，10～20年と長期間稼働するものである。また，設置される環境も様々である。これらの装置の傍らに設置されるIoTゲートウェイ装置には，長期間の安定動作を実現する長期信頼性設計と，過酷な環境にも設置できる耐環境設計が求められる。更に，ネットワークを介した不正アクセスだけでなく，USB (Universal Serial Bus) ポートなどの外部インターフェースからの侵入や，直接装置の内部にアクセスされたり装置を分解されたりするような脅威に対しても，堅牢でなければならない。

3　SPINEX™のエッジコンピューティングを実現するソフトウェア

当社は，インダストリアルIoTのエッジ層が備えなければならない柔軟性，適用性，及び拡張性を実現するために，ソフトウェア定義によってエッジの処理やネットワーク構成を自在に構築できるSDEN (Software Defined Edge Network)，IoTクラウドハブ，及びデータ処理や，イベント検知，圧縮送信，

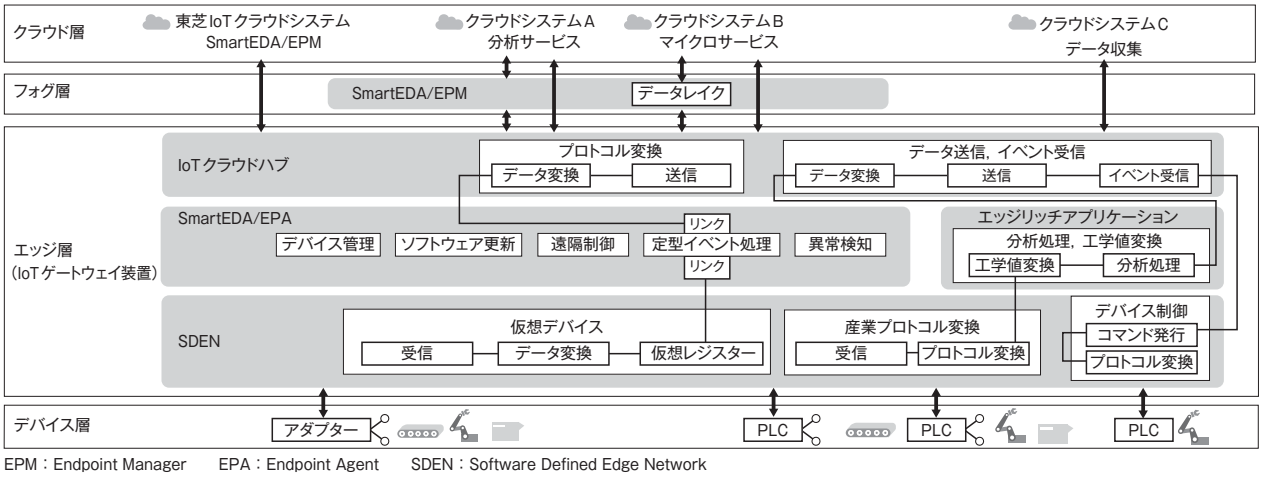

図1. SPINEX™のエッジアーキテクチャー ― 装置の各種プロトコル，データ形式，エッジリッチアプリケーション，及びマルチクラウドとの柔軟な接続を可能にした。

SPINEX IoT architecture for edge computing

接続デバイスの制御などのインテリジェントな処理をエッジ側で行うSmartEDA/EPA（Endpoint Agent）から成るエッジアーキテクチャーを構築した（図1）。

SDENは，様々なセンサーデバイス，PLCや各機器のプロトコル，及びデータ構造の違いを吸収し，それらを容易に接続して自由に変更でできるように，ノード（処理）とそれらを複数連結したフロー（流れ）で構成した。このノードとフローによって，様々なエッジデバイスを抽象化し，共通のインターフェースを持つ仮想デバイスとして定義することで，上位の生産システムから統一して管理できる。

また，エッジ層には，工作機械やロボットなどで遅延に対する要求が厳しいデータの処理と応答が求められるイベント処理，及びエッジリッチアプリケーションをプラグインとして実装し，インテリジェントな処理を容易に実現できるようにした。

IoTクラウドハブは，クラウドシステム側との接続で，同様にソフトウェア定義によってデータ構造の変換や適切なプロトコルノードを選択し，複数のクラウドシステムやクラウドサービスが接続できるハブとして機能する。

このエッジアーキテクチャーを実現するために，プラットフォームに依存しない実行可能なJavaScript言語で記述し，そのJavaScriptで記述したノードを複数連結して，フローを構成するオープンソースのNode-RED(注1)をベースにした。これらによって，装置内部のバイナリープログラムを変更することなく，ユーザー自身でエッジ処理の処理内容を構成できるようになった。下位機器との接続には各種産業用プロトコル（Modbus/TCP（Transmission Control Protocol），OPC UA（Unified Architecture)[1]など）に対応したノードを，また上位クラウドシステムとの接続には各種クラウドシステムに対応した通信プロトコル（MQTT（Message Queuing Telemetry Transport），HTTPS（Hypertext Transfer Protocol Secure），Web Socket，及びAMQP（Advanced Message Queuing Protocol））ノードを用意し，SmartEDA/EPAのイベント処理ノードとリンクして，柔軟性を持ったエッジリッチコンピューティングを実現した。

4　IoTゲートウェイ装置

IoTゲートウェイ装置の開発にあたり，社会インフラ・産業分野に求められる各種要件を，ユースケース検討で抽出し，装置仕様に落とし込んだ。今回開発したIoTゲートウェイ装置の主な仕様を**表1**に示す。

4.1　耐環境設計と長期信頼性設計

耐環境設計を考えるときにIoTゲートウェイ装置の温度仕様と振動・衝撃仕様が，重要なファクターとなる。温度仕様については，筐体（きょうたい）自体をヒートシンク構造とし，CPUやメモリーなどの主要な発熱部品を直接筐体に接触させて放熱する部品配置を採用することで，ファンレス設計による長期信頼性の確保と温度仕様を両立させる工夫を行った。また，耐振動・衝撃 については，CPU周辺への補強板金の配置や，メモリーチップやフラッシュROMなどの高密度BGA（Ball Grid Array）部品への接着剤の塗布により，部品への機械的ストレスを軽減させる工夫や，機械的ストレスが掛かる位置への主要部品の配置禁止を行った。

長期信頼性の実現については，上記の耐環境設計に加え，熱ストレスによってはんだ接合部に生じるクラックの影響を最小限に抑えるために，車載向け基板で実績のある部品実装パッドを採用し，電解コンデンサーや冷却用ファンなどの有寿命部品を排除した。フラッシュストレージデバイスには，データを長期間保持するための定期的なデータリテンション機能を実装した。更に上記対策の有効性を確認するために，熱応力シミュレーションによる解析や，TCT（Thermal Cycle Test），HALT（Highly Accelerated Life Test）などの信頼性試験を実施し，IoTゲートウェイ装置としての長期信頼性を確保した。

4.2　セキュリティー脅威への対応

近年，制御システムへのサイバー攻撃の脅威が増大しており，サイバー攻撃のリスクを低減する手法として，制御システム

表1．IoTゲートウェイ装置の要件と主な仕様
Performance requirements and main specifications of newly developed IoT gateway device

項　目		要　件	仕　様
CPU	コア数，キャッシュ	処理性能 ミリ秒オーダーで複数センサー（～10個）のエッジ処理を同時に実行可能であること	4コア，L2キャッシュ（2Mバイト）
	周波数		1.6 GHz
メモリー	DRAM		8Gバイト
	フラッシュ		28.8 Gバイト
3G/LTE		インターフェース 想定されるエッジデバイス（PLC，通信アダプター，旧型工作機械）とのデータ通信が可能であること。 上位装置（クラウドサーバー，フォグサーバー）への有線・移動体通信が可能であること	1（オプション）
イーサネット			2（10BASE-T/100BASE-TX/1000BASE-T）
USB			2（USB3.0）
COMポート	RS232		1（切り替え）
	RS485		
拡張ボードスロット	mSATA		1（オプション）
	A-I/D-IO		1（オプション）
環境条件（動作時）	温度	耐環境性 想定される設置環境（工作機械や，社会インフラ機器，鉄道など）に求められる仕様を満足すること	−25～+60℃
	湿度		10～90％
	振動，衝撃		車載JIS C 60721-3-5，鉄道JIS E 5006
入力電源		DC（直流）入力があること	DC 12−36 V
OS，エッジソフトウェア		SPINEX™アーキテクチャーのエッジソフトウェアであること	Linux，SDEN，IoTクラウドハブ

3G：第3世代　LTE：Long Term Evolution
mSATA：mini Serial Advanced Technology Attachment
A-I：Analog Input　D-IO：Digital Input Output
JIS：日本工業規格　OS：基本ソフトウェア

（注1）　ハードウェアデバイスAPI（Application Programming Interface），及びオンラインサービスを接続するためのツール。

分野におけるセキュリティー標準規格であるIEC 62443（国際電気標準会議規格 62443）シリーズが注目されている。今回，IoTゲートウェイ装置の開発にあたっては，その設置条件やデータアクセス方法などのユースケースを検討した上で，必要とされるセキュリティー要件をIEC 62443シリーズから抽出し，それらを具体的にゲートウェイ装置で実現する方法を検討して実装した。

IoTゲートウェイ装置の主なセキュリティー要件としては，物理アクセス保護や，デバッグポートの無効化，セキュアブート，ホワイトリスティング，暗号鍵のハードウェア保護などがある。

物理アクセス保護については，USBやCOM（シリアル通信）ポートなどの外部インターフェースからの不正物理アクセスを防止するために，BIOS（Basic Input Output System）で当該ポートをディセーブルに設定する機能の実装と，CPUやメモリーなどの主要部品に物理的に直接プロービングできないように配線を内層化する工夫を行った。

デバッグポートの無効化については，UART（Universal Asynchronous Receiver Transmitter）などのデバッグ用ポートを不必要にユーザー開放しないように，アクセス用の信号ピンを立てないことや，信号を表すためのシルク表記の削除，出荷時にBIOSで当該ポートをディセーブルに設定する機能の実装などで対応した。

セキュアブートについては，セキュアブート対応OS（基本ソフトウェア）の起動に必要となるデバイス固有暗号鍵情報をIoTゲートウェイ装置内のTPM（Trusted Platform Module）デバイスに保存し，OS起動時に当該固有暗号鍵を参照する仕組みを実装した。これにより，OSがインストールされたストレージが万一盗難された場合にも，他機器からのブートやデータ参照を阻止できる。

5　適用システム例

製造工場に設置されている各種工作機械のデータを収集し，これらの見える化と異常予兆の検知をはじめとした分析を行うシステムの例を，**図2**に示す。工場内には，製造工程ごとに工作機械やロボットのような製造装置や，製造装置を動かすためのコンプレッサーなどの動力源が設置されている。これらの装置からの各種出力データや，追加したセンシングデバイスからのデータを，IoTゲートウェイ装置が収集して一次処理した上で，工場内フォグサーバーに送信する。

各装置の出力データの異なるインターフェース仕様やプロトコルは，SDENであらかじめ用意しておいたノードで吸収し，工場内フォグサーバーのアプリケーションがプロトコルの違いを意識しなくてもよいようにした。既設PCサーバーによるローカルなデータ収集は処理に変更を加えることなく，SDENによってネットワーク化した。また，スマートファクトリーのデータ交換標準として期待されているOPC UAもSDENによって段階的に対応し，進化できるようにした。

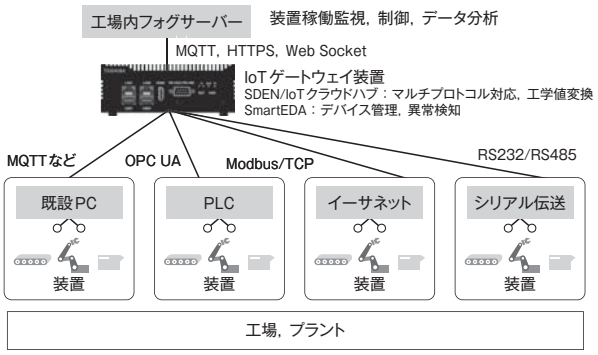

図2．製造工場システムへのIoTゲートウェイ装置の適用例 — 工作機械の稼働情報と，工作機械に取り付けたセンサーからの異常診断情報を，IoTゲートウェイ装置に集約して分析し，工場内の監視・制御アプリケーションに送って異常予兆の見える化を行う。

Example of application of newly developed IoT gateway device to manufacturing facility

6　あとがき

マルチデバイスとマルチクラウドで構成されるインダストリアルIoTのエッジコンピューティングを，ソフトウェア定義によって柔軟に構成し進化させられる仕組みを持ち，かつ耐環境性，長期信頼性，及びセキュリティー脅威に対する堅牢性を備えたIoTゲートウェイ装置を開発した。

今後，メディア処理やAIなどのインテリジェントな処理を組み込んだエッジリッチコンピューティングに発展させ，新たな付加価値を創造していく。

文　献

(1) Mahnke, W. et al. OPC Unified Architecture. Berlin, Springer-Verlag, 2009, 339p.

中嶋　　宏　NAKAJIMA Hiroshi
東芝デジタルソリューションズ（株）
ICTインフラサービスセンター IoT設計部
Toshiba Digital Solutions Corp.

松本　賢一郎　MATSUMOTO Kenichiro
東芝デジタルソリューションズ（株）
ICTインフラサービスセンター IoT設計部
Toshiba Digital Solutions Corp.