



家庭から宇宙まで、エコチェンジ



三菱電機技報

7

2016

Vol.90 No.7

IoTを支える情報・通信技術



目 次

特集「IoTを支える情報・通信技術」

データ共有が生み出す新たな価値……………	巻 頭 言 1
稲田修一	
IoTが実現する未来社会……………	巻頭論文 2
早川孝之	
IoTプラットフォームのアーキテクチャ……………	7
田村孝之・塚本良太・原田篤史・渡邊和樹	
海外におけるEMSソリューション……………	12
滝田大介・京屋貴則・飯島昌平・大塚 晃	
イベント向け警備支援のための映像解析技術……………	16
宮城惇矢・西辻 崇・服部亮史・古木一朗	
ホームネットワークの進化とIoT……………	21
三木智子	
高信頼・低遅延な無線通信技術……………	25
青山哲也・鈴木和雅・梅田周作・木下裕介・武 啓二郎	
IoTを支えるイーサネット規格TSN技術……………	30
堀田善文・谷口幸子・川手竜介・マンジン クリストフ	
IoT時代のセキュリティ技術……………	35
米田 健	
設備維持管理向けデータ分析技術……………	40
平井規郎・中村隆顕・増崎隆彦・栗山俊通・上田宜史	
高性能センサデータベース……………	45
郡 光則・米田貴雄	
大規模IoTシステムにおける 計算機リソースサイジング技術……………	50
魚住光成・小杉 優・佐藤尚也・鶴 薫	

Information and Communication Technologies of IoT

Value Creation through Data Sharing Shuichi Inada
Future Society Realized by IoT Takayuki Hayakawa
Architecture of an IoT Platform Takayuki Tamura, Ryota Tsukamoto, Atsushi Harada, Kazuki Watanabe
EMS Solutions in Overseas Market Daisuke Takita, Takanori Kyoya, Shohei Iijima, Akira Otsuka
Visual Analysis Techniques for Event Security Management Junya Miyagi, Takashi Nishitsuji, Ryoji Hattori, Ichiro Furuki
Evolution of Home Network and IoT Satoko Miki
Reliable and Low-latency Technologies for Wireless Communication Tetsuya Aoyama, Kazumasa Suzuki, Shusaku Umeda, Yusuke Kinoshita, Keiji Take
Ethernet-based Time Sensitive Networking Technologies for IoT Yoshifumi Hotta, Sachiko Taniguchi, Ryusuke Kawate, Christophe Mangin
Information Security Technologies in the Age of IoT Takeshi Yoneda
Data Analysis Technologies for Maintenance and Management of Facilities Norio Hirai, Takaaki Nakamura, Takahiko Masuzaki, Toshiyuki Kuriyama, Takafumi Ueda
High-performance Sensor Database Mitsumori Kori, Takao Yoneta
Computer Resource Sizing Technology in Large-Scale IoT Systems Mitsunari Uozumi, Yu Kosugi, Naoya Sato, Kaoru Tsuru

特許と新案

「経路制御方法、通信システム、無線端末および ゲートウェイ端末」……………	55
「自己認証通信機器および機器認証システム」……………	56
「通信システム、局側光回線終端装置、利用者側 光回線終端装置、制御装置、並びに通信方法」……………	56



表紙：IoTを支える情報・通信技術

三菱電機は、機器をネットワークで結び、情報技術によって新たなソリューションを生み出すIoT(Internet of Things)を支える技術開発に取り組み、未来社会に貢献していく。機器から得られる大量な情報を、確実にかつ安全に収集し、高度な分析に基づいたサービスで生産性向上や利便性向上といった価値を創出する。

表紙の写真は、IoTが創る快適かつ安全・安心な未来社会をイメージで示した。

巻/頭/言

データ共有が生み出す新たな価値

Value Creation through Data Sharing



稲田修一
Shuichi Inada

データを共有し、価値創造につなげる取り組みが加速度的に広がり始めている。例えば、稼働管理である。顧客サイドにある機器をネットワークにつないでデータを収集し、それを分析し価値を創造する仕組みを作る。現場では個々の顧客にカスタマイズした形で価値を提供し、保守・運用を最適化する。データ活用を担当する部門と営業・保守拠点、場合によっては顧客までもがデータを共有することによって、新しい価値を創造しているのである。

ドイツ産業界が主導するインダストリー4.0でもデータ共有がポイントになっている。ここでは設計、開発、生産計画、生産、サービス提供などバリューチェーン全体をつなぎ、価値創造に必要なデータを、業界の垣根を超えて複数企業が共有する。

この“共有”という概念は、21世紀における社会や人の価値観の大きな変化を反映している。シェアリングエコノミー（共有型経済）の普及はその表れで、カーシェアやホームシェアにとどまらず、多岐にわたるモノのレンタルなど製品のシェア、介護・保育などサービスのシェア、社会や投資に必要なお金のシェアなど、さまざまな分野で新しいビジネスが立ち上がっている。

この概念は、資源の有効活用やフェアな価値評価につながる。また、協働や共創などネットワーク型の価値創造にも根源的なところでつながっている。そして、これを容易にしたのは、インターネットを始めとする情報通信手段の発展である。データ共有の広がりは、まさにこのような社会全体の大きな変化の中で起こっている事象なのである。

しかし現実に立ち戻って考えると、データ共有は簡単ではない。現場では“データは門外不出”という考え方が製造業を中心に根強い。でも、このような伝統的な考え方を変えることがイノベーションにつながる。企業間をまたがるサプライチェーン全体の最適化はその1つである。

また、市場ニーズの変化や将来の売行きを予測し、それを製品やサービスの企画・開発・生産にフィードバックする仕組みも活発化している。この実現には、市場サイドと

生産サイドのデータ共有が必要である。

データが持つ性質も共有化を促進する。それは、規模と範囲の経済性である。分析するデータの範囲や精度・粒度、分析手法などが同じならば、データ活用の価値はデータ量に依存する。実際、業界下位企業からは上位企業に勝てないとの悲鳴が聞こえてくる。この解決策の1つは、ライバル企業とデータを共有することである。

範囲の経済性に関しても、共有によってこれを実現する取り組みが行われている。ネット店舗と実店舗でデータを共有する、異業種企業とデータを共有するなどの取り組みである。例えば、レシピの検索データを持つ企業がスーパーとデータ共有している。レシピ検索のデータを活用すると、食材の売上げを増やすことができる。逆に、食材の購入データから実際に作られる料理を推測することによって、レシピのおすすめ精度をあげることができる。Win-Winの関係が成り立つのである。

データ共有は価値創造の有力な手段である。でも、誤解してはほしくないことがある。共有のため何でもオープンにすれば良いと考えるのは大きな間違いだ。オープンかクローズか、誰にどこまでオープンにするのか、そのメリットとデメリットをきちんと評価し、戦略的に行うことが必要なのである。

日本企業は技術に関しては、オープン・クローズ戦略の重要性に気づき、技術戦略の一環としてこれに取り組み始めているが、データに関しても、同じ目線で考えることが必要である。

これからの時代は、“知”の集積が企業の国際競争力に大きく影響する。そのベースになるのは、集積したデータから得られる情報や知識である。技術と同様、データの集積には時間がかかる。早期にこれに取り組み、組織としてデータの共有や活用が当たり前という文化や風土を構築すること、これが21世紀のエクセレント・カンパニーに求められる必要条件の1つである。



早川孝之*

IoTが実現する未来社会

Future Society Realized by IoT

Takayuki Hayakawa

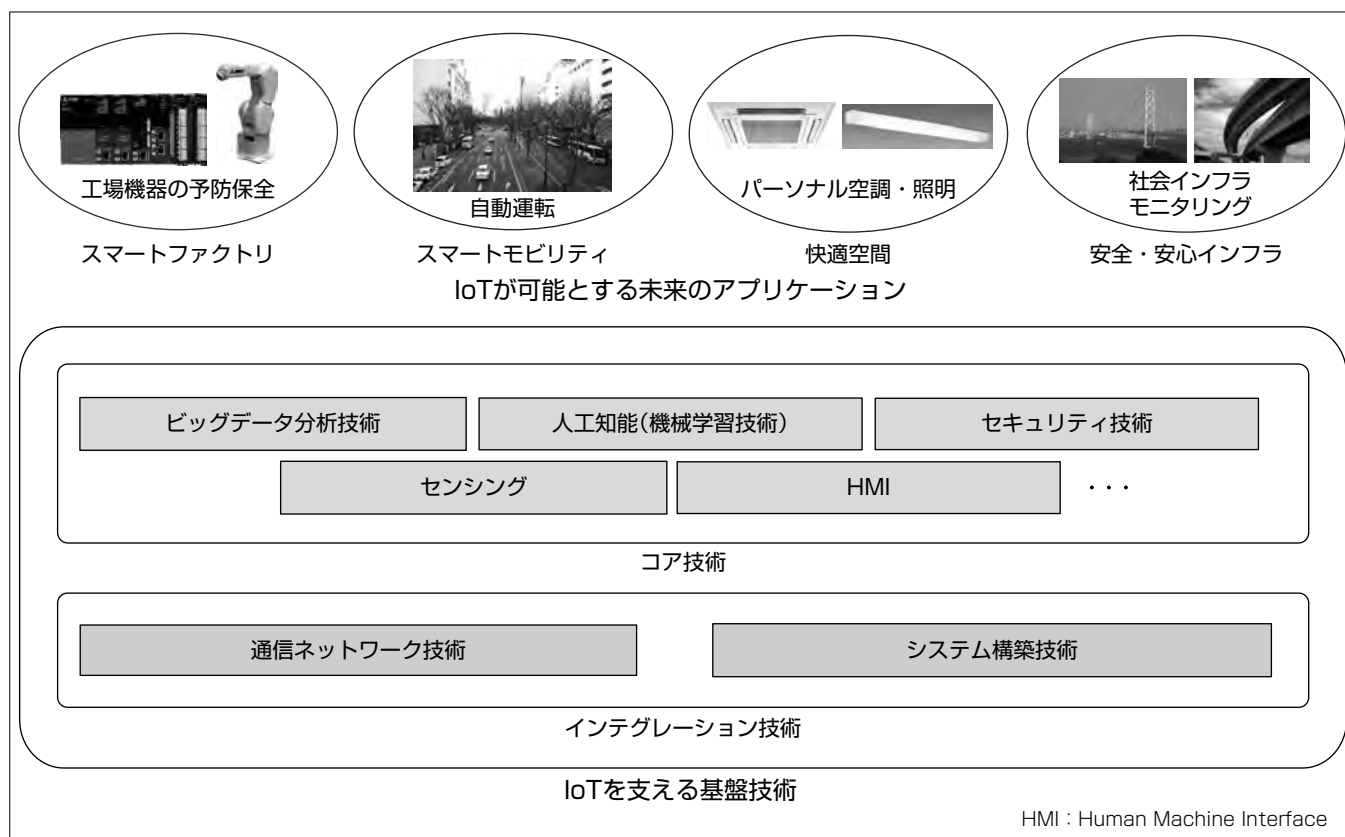
要 旨

IoT(Internet of Things)を支える基盤技術に対する三菱電機の出組みを俯瞰(ふかん)する。IoTがもたらす未来の例として、IoTが可能にする未来のアプリケーションであるスマートファクトリ、スマートモビリティ、快適空間、安全・安心インフラが挙げられる。

当社は、これらの未来を実現するIoTを支える基盤技術の開発に取り組んでいる。当社のIoTを支えるコア技術の戦略は、“エッジコンピューティング”と“ハードウェア技術とITの融合”を特徴とする。エッジコンピューティングによって、現場の機器や現場近くに設置される組み込み計算機でデータ処理を行うことで、迅速な課題解決や、ノウハウ等の機密性が高い情報の保護が可能となる。ハードウェア技術とITの融合によって、ハードウェアの理解に基づ

くデータ分析を行うことで、一段レベルの高い分析結果を得ることが可能となる。この戦略に基づくコア技術として、ビッグデータ分析技術、人工知能(機械学習技術)、セキュリティ技術、センシング、HMI等がある。また、インテグレーション技術として通信ネットワーク技術とシステム構築技術がある。

IoTがもたらす未来は、生産性向上、ユーザーの利便性向上といったメリットを産業・社会等へもたらすことが期待される。一方で、収集される情報範囲の拡大、情報システムによる実世界のモノの制御範囲の拡大などによって、新たな課題が発生すると考えられる。当社は、これらの課題解決に資する、IoTがもたらす未来の実現に必要な基盤技術の開発に引き続き取り組んでいく。



IoTを支える基盤技術に対する取組み

生産性向上、ユーザーの利便性向上といったメリットを産業・社会等へもたらすことが期待される。IoTによる未来のアプリケーションを実現するため、IoTを支えるコア技術としてビッグデータ分析技術、人工知能(機械学習技術)、セキュリティ技術、センシング、HMI等、また、インテグレーション技術として通信ネットワーク技術、システム構築技術に取り組んでいる。

1. ま え が き

本稿では、IoTを支える基盤技術に対する取組みを俯瞰する。最初に、IoTがもたらす未来の例として、IoTが可能にする未来のアプリケーションであるスマートファクトリ、スマートモビリティ、快適空間、安全・安心インフラを説明し、次に、当社におけるIoTを支える基盤技術に対する取組み内容を述べる。

2. IoTがもたらす未来

世の中のメガトレンドとして、情報化の進展、人口構造の変化、急速な都市化の進行、気候変動・省エネルギー対策の遅延、世界情勢の変化が挙げられる。メガトレンドから生じる課題として、先進国の高齢化、都市部の渋滞、地球温暖化、エネルギー不足、自然災害が存在する。これらの課題解決に貢献する、IoTが可能にする未来のアプリケーションの例として、スマートファクトリ、スマートモビリティ、快適空間、安全・安心インフラの4つを次に述べる。

2.1 スマートファクトリ

スマートファクトリは、工場内の機器を情報システムにつなげ、データの分析や最適化を行うことで、生産効率向上や省エネルギー化を実現するアプリケーションの総称である。スマートファクトリの具体例を次に述べる。

工場機器の予防保全

工場機器の予防保全は、工場機器から得られるデータを分析することで工場機器の障害発生を予測し、本当に保守が必要な機器だけに対して、事前に保守管理を行うことが可能とする。予防保全によって、保守コストの低減、工場ラインの稼働率向上による生産効率向上が期待される。

設計・製造プロセスの最適化

製品の設計段階で、コンピューターシミュレーションを活用してコンピューターの中の仮想世界における試行錯誤を繰り返し、製造プロセスも考慮した設計を行うことで、設計・製造プロセスを最適化する取組みが行われている。この取組みにIoTを組み合わせ、現実世界で得られるデータによるフィードバックをかけることで、より高い精度のコンピューターシミュレーションによる検証や、より良い設計品質の実現が期待される。

2.2 スマートモビリティ

スマートモビリティは、環境に優しい、つながりあう移動手段を実現することで、都市部の渋滞解消、省エネルギー化、高齢者の移動容易化を図るアプリケーションの総称である。スマートモビリティの具体例を次に述べる。

自動運転

自動運転は、加速・操舵・制動のいずれかをシステムが行うレベル1から、それら全てをシステムが行い、ドライ

バーが全く関与しないレベル4までの4段階に分類され⁽¹⁾、自動車メーカーだけでなくGoogle等のIT企業も2020年頃の実用化を目指して開発を進めている。

法制度上の課題はあるが、完全自動走行が実現すると、高齢者など自分で運転できない人も自動車で自由に移動が可能となる。また、自動運転車の走行経路を適切に制御することで、都市部の渋滞解消につながることも期待される。加えて、自動運転の安全性能が向上することで、交通事故を減らせることが期待される。

さらに、近年広がりを見せている自動配車システムやカーシェアリングの考え方と自動運転を組み合わせることで、自動車を社会で共有する一種の公共交通機関として活用し、社会全体の省エネルギー化につながることも期待される。

2.3 快適空間

快適空間は、利用者一人ひとりにあわせた家、ビルの快適性を追求しながら、持続可能な社会のための環境配慮にも対応するアプリケーションの総称である。快適空間の具体例を次に述べる。

パーソナル空調・照明

オフィスでの人の在席状況に応じて、空調や照明のオン・オフ制御を行う空調・照明制御システムは既に実用化されている⁽²⁾。在席状況だけでなく、外気温や天気といった外部環境と、在席者の身体の状態・作業内容も考慮することで、快適性の向上と省エネルギー性を両立させる空調・照明制御が実現可能になると期待される。

2.4 安全・安心インフラ

安全・安心インフラは、人が安全で安心に暮らすことができる社会を実現するため、道路・鉄道・橋梁(きょうりょう)などの社会インフラ設備の維持管理や、集中豪雨などによる自然災害発生の監視を実現するアプリケーションの総称である。安全・安心インフラの具体例を次に述べる。

社会インフラモニタリング

橋梁やトンネルといった社会インフラ設備は、建設後年数が経過するに従い劣化が生じ、橋の崩落やトンネルの天井落下による事故発生や交通路遮断が起きる危険性が高まる。現状は、人が定期的に検査をして劣化状況を判断し、必要場合は補修を行うことで対処しているが、劣化状況見逃しによる事故が発生している。これに対して、社会インフラ設備の状態を計測するセンサの設置や、センサを搭載した自動車による社会インフラ設備近辺の走行⁽³⁾で、社会インフラ設備の状態データを収集し、収集したデータと社会インフラ設備の利用状況を分析し、劣化状況判断や予知保全を行うことで、検査の省力化と補修対策の効率化が実現され、事故を未然に防ぐことで安全・安心性が高まることが期待される。

3. IoTを支える基盤技術への取組み

当社のIoTを支えるコア技術の戦略は、“エッジコンピューティング”と“ハードウェア技術とITの融合”を特徴とする。エッジコンピューティングによって、現場の機器や現場近くに設置される組み込み計算機でデータ処理を行うことで、迅速な課題解決や、ノウハウ等の機密性が高い情報の保護が可能となる。ハードウェア技術とITの融合によって、ハードウェアの理解に基づくデータ分析を行うことで、一段レベルの高い分析結果を得ることが可能となる。この戦略に基づくコア技術(ビッグデータ分析、人工知能、セキュリティ)と、インテグレーション技術(通信ネットワーク、システム構築)への取組みを次に述べる。

3.1 ビッグデータ分析技術

機器のビッグデータを用いたデータ分析技術には、大量のデータが扱えること、高速に分析できることが要求される。一方で従来の統計処理的分析技術は、少量のデータから全体像を推定することを目的としていたため、ビッグデータ分析に対しては必ずしも有効な手段ではないものがあつた。そこで、当社はこれらの課題を解決するため、大量のデータを扱い、かつ高速に処理することが可能な分析技術として、パターン検知技術とデータ特徴可視化技術を開発した。次に2つの技術について述べる。

パターン検知技術

この技術は時系列データから異常状態を自動で検知するための技術である。異常検知技術には大きく分けて重回帰分析と時系列データ分析の2つの技術がある。前者はデータの安定的な相関性を監視し、それが不安定になったときに異常と判断するもので、古くから異常検知に使われてきた技術である。この技術の短所は相関性がない場合に使えないこと、また複数のデータ項目を組み合わせる分析することから、計算量が膨大になるため、大量データを扱うのが困難であることが挙げられる。そこで、時系列データに表れる一定のパターンを抽出し、そのパターンがくずれていないかどうかを監視することで高速に異常を検知する技術を開発した(図1)。

データ特徴可視化技術

この技術はデータを分析する人を支援するための可視化技術である。データを分析する人には、思考が途切れることなく様々な視点から高速にグラフを切り替えながら分析

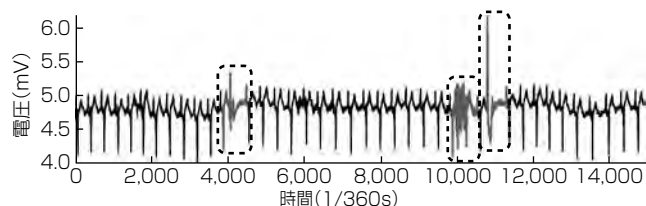


図1. パターン検知技術による異常検知例

することが求められる。また、ビッグデータでは分析対象が膨大になるため、可能な限り試行錯誤の回数を軽減することが重要である。これらに対する解決策として、大量のデータを高速にグラフ表示し(1秒で300万件)、グラフの切り替えを容易にし、分析すべき箇所を強調表示して分析者の試行錯誤の回数を軽減(通常の1/4程度)することで、分析者を支援する技術を開発した(図2)。

3.2 人工知能(機械学習技術)

安全・安心・快適な社会の実現に向けて、人工知能市場は、今後ますます成長すると予測されている。また、センサデバイス技術やネットワーク技術の発達によって、リアルタイムに大量のデータを取得できるようになっている。しかし、大量のデータをサーバに集約して人工知能による推論処理を実行しようとする、サーバやネットワークの設備が大規模化するため、コストは上昇する。また、機密情報のアップロードに対するセキュリティ対策やネットワーク遅延・障害への対策が必要になる。そこで、大量のデータをサーバに集約しなくても高度な推論ができる人工知能技術が求められている。

当社は、組み込み機器に搭載可能な“コンパクトな人工知能”を開発している。これによって、従来サーバで行っていた高度な推論を、車載機器や産業用ロボット、工作機械などの組み込み機器でもできるようになり、安全・安心・快適な社会の実現に貢献可能となる。

(1) 推論処理の少演算量・省メモリ化による人工知能のコンパクト化

人工知能の一種で“深層学習”と呼ばれる機械学習アルゴリズムは高度な推論が可能であるが、多層のネットワーク構造を用いて推論するため、推論処理に必要な演算量・メモリ量が膨大になる。このため、ネットワーク構造と計算方法を効率化する新たなアルゴリズムを開発した。これによって、従来の推論の精度は保ったまま人工知能のコンパクト化が可能になった。例えば、画像認識では、演算量・使用メモリ量を90%削減(当社比較)できる。

(2) 人工知能の組み込み機器への搭載による利用範囲の拡大

“コンパクトな人工知能”によって、組み込み機器で高度な推論が可能になる。例えば、車載機器に搭載すればドラ

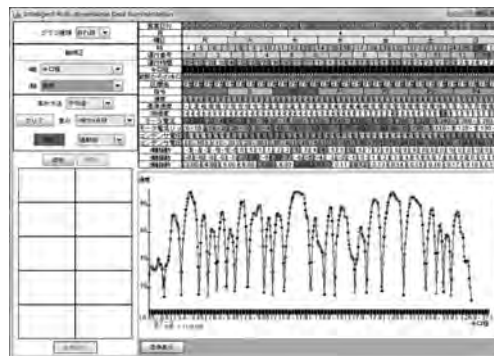


図2. データ特徴可視化技術による可視化例

イバーの普段の運転から漫然運転が検知可能となり、工作機械に搭載すれば工場現場での人の作業分析ができるようになる。大量のデータをサーバに集約して処理していた従来の方法と比べ、サーバやネットワーク設備の小規模化によって人工知能導入のコストが抑えられる。さらに、機密情報をサーバにアップロードする必要がないため高いセキュリティ環境を構築できる。また、組み込み機器で推論処理することで、推論の際にネットワークを介するの必要がなくなる。このため、ネットワーク環境に依存せずに高速処理ができ、機器ごとの環境に応じた適切な推論も可能となる。今後、自動車機器、FA機器、監視カメラなどへの搭載が見込まれ、将来的にはIoT社会を支える基盤技術にしたいと考えている。

3.3 セキュリティ技術

近年、IoTの進展によってネットワークを介したサイバー攻撃による機密情報の漏洩(ろうえい)や重要インフラの機能不全のリスクが高まっている。また、米大統領が2015年9月の米中首脳会談で中国のサイバー攻撃に懸念表明する等、サイバー攻撃は国家レベルの課題となった。日本政府もサイバー攻撃対策への取組みを本格化するためのサイバーセキュリティ基本法を2015年1月に施行し、内閣に“サイバーセキュリティ戦略本部”を、内閣官房に“内閣サイバーセキュリティセンター(NISC)”を設置し、サイバーセキュリティ対策の立案・遂行が積極的に推進されている。日本政府は、企業に対して主に①サイバー攻撃情報の共有、サイバー攻撃を検知・防御する組織の構築と組織間の連携、②製品開発・運用プロセスのセキュリティ基準・ガイドライン策定・遵守促進、③第三者による製品・システム・組織のセキュリティ認定の取得促進、④攻撃検知・防御技術、暗号技術の研究開発促進の取組み強化を求めている。

当社はこれらの取組みを強化中である。次に攻撃検知・防御技術と暗号技術の研究開発への取組みとして、機器のセキュリティ、ネットワークのセキュリティ、データのセキュリティの取組みについて述べる。

(1) 機器のセキュリティ：LSIの指紋

2020年には500億個の機器がネットワークにつながると言われており、各機器をウイルスの混入から守ることが重要な課題となる。この課題を解決するのがLSIの指紋である⁽⁴⁾。LSIの指紋は、LSIの製造ばらつきを利用してLSIの固有IDを生成する技術である。LSIの分解やLSI回路の複写といった強力な攻撃から固有IDの漏洩を防止できるといった特長を持つ。LSIの指紋を既存の公開鍵暗号や共通鍵と組み合わせて利用することで、機器に対する安全なソフトウェア更新や機器の認証が実現できる。

(2) ネットワークセキュリティ：手口に着目した攻撃検知

近年、大きな情報漏洩をもたらすサイバー攻撃は、メールに添付されたウイルスへの感染が原因である。ウイルス

は年間3億種の新種が発生しており、過去のウイルスと一致するウイルスを見つける手法では検知が困難となっている。この課題を解決するため、個々のウイルスではなく、ウイルスを用いた攻撃者の手口に着目して攻撃を検知する方法を開発した⁽⁵⁾。分析の結果、攻撃者の手口は50程度であることを解明し、手口に注目することで効率的な攻撃検知を実現可能とした。

(3) データのセキュリティ：秘匿検索

IoTの時代には、人や機器の情報をクラウドに収集して分析するビッグデータ処理によって、付加価値創出が期待される。しかし、人や機器の情報は、機密性が高くクラウドに保存する場合には暗号化が求められる。一方、従来、暗号化された情報を検索する場合、一旦クラウドで復号する必要があり、その際に情報が漏洩する懸念があった。そこで、クラウド上での復号処理なしで検索できる暗号を開発した⁽⁶⁾。この技術によって、情報の秘匿と活用の両立が実現できる。

これらの機器・ネットワーク・データのセキュリティ技術によって、安全安心な社会実現への貢献を目指す。

3.4 通信ネットワーク技術

当社は、IoTを支える通信ネットワーク技術として、様々な機器をシステムにつなげるためのフィールドネットワークに向けた有線通信と無線通信の技術開発に取り組んでいる。

有線通信技術では、Ethernet^(注1)技術をベースとした、低遅延と高信頼化を実現するTSN(Time Sensitive Networking)の標準化がIEEE 802委員会で行われている。Ethernetは、既にパソコン等の通信インタフェースとして普及しており、Webアクセス等で汎用的に使われるIP(Internet Protocol)通信と親和性が高い。TSNの標準化では、従来個別のネットワークで接続されていた車載機器や産業機器を、IP通信によるインターネットサービスにシームレスに接続し、かつ、車載や産業分野で要求される低遅延時間での転送を実現するため、Ethernetに対する遅延性能改善や高信頼化に必要な機能追加を行う予定である。当社は、TSNに基づくEthernet転送技術の開発に取り組んでいる。

無線周波数には、無線局の免許が必要なライセンスバンドと免許が不要なアンライセンスバンドがある。自動車や鉄道、ビルや工場、橋などの社会インフラを対象として、設置利便性やリアルタイム性、信頼性を確保するには、ライセンスバンドとアンライセンスバンドそれぞれを用途によって使い分けるとともに、高信頼・低遅延化技術の適用が必要となる。当社は、鉄道や高速道路等の高速移動体を対象として、リニアセル構築技術、無線LAN等のアンライセンスバンドを用いる機器からの耐干渉性を高めた耐干渉無線技術といった高信頼・低遅延化技術の開発に取り組んでいる。また、広範に普及して様々な端末・デバイスが利用している無線LANに関して、マルチホップ

機能によってネットワーク配線を不要とした無線LANアクセスポイントに、バッテリーを組み合わせることで電源配線も不要とし、簡易又は一時的なネットワーク構築を可能にすることで利用シーン拡大を目指した開発を行っている⁽⁷⁾。920MHz帯特定小電力無線は、電波が届きやすく、消費電力が小さい特長を活用して、スマートメータ、家庭、工場、ビル、公共インフラ等、様々な分野への活用が期待される。920MHz帯特定小電力無線に関して、自動検針や宅内電力の見える化に加え、デマンドレスポンスにも対応可能なスマートメータの通信ネットワーク技術の開発を行っている⁽⁸⁾。

(注1) Ethernetは、富士ゼロックス(株)の登録商標である。

3.5 システム構築技術

IoTシステムの構築では、Web／アプリケーションサーバ、ゲートウェイ(GW)、及び端末上で連携して動作するソフトウェアの開発が必要になる。それぞれの構成要素は処理能力が大きく異なり、構成要素間の通信経路にも速度や品質に差があるため、機能の分散配置や障害耐性等、ソフトウェア設計時に考慮すべき事項が多い。アプリケーションごとにソフトウェアスタック全体を設計するのは非効率的であり、共通的な機能を抽出して部品化することが重要となる。図3にこの方針に基づくIoTシステムの全体構成例を示す⁽⁹⁾。

機器が送信するデータを利用するサーバアプリケーションに対しては、クラウド上でデータを受信し、データベースに格納する処理を仮想サーバ単位でM2M(Machine to Machine)サーバとして部品化する。データベースはKVS(Key-Value Store)型とし、任意の機器データをデータ型名とともに記録することで、データ変換等の処理の詳細を柔軟に変更可能とする。処理効率が問題になる場合は、変

換結果を別の関係データベースシステムに格納して利用する。

また、機器に対して要求を送信するサーバアプリケーションに対しては、機器をインターネット上に公開することなくクラウドサーバとの双方向通信を可能にするメッセージ中継機能(ブローカ)を部品化する。

IoTシステムには、接続機器数や端末数の増加に対応するスケーラビリティが求められる。そこで、上記データ受信やメッセージ中継機能は、M2Mサーバの増設によってスケールアウト可能な設計としている。

当社では、これらの方針に基づくPaaS(Platform as a Service)環境“DIAPLANET”を提供している⁽¹⁰⁾。

4. む す び

IoTがもたらす未来の例と、IoTを支える基盤技術に対する当社の取組み内容を述べた。IoTの社会実装に資する標準化に向けて、ISO/IEC JTC1、IIC等複数団体が活動しており、技術開発に加えて標準化の取組みも進めていく。IoTがもたらす未来は、生産性向上、ユーザーの利便性向上といったメリットを産業・社会等へもたらすことが期待される。一方で、収集される情報範囲の拡大、情報システムによる実世界のモノの制御範囲の拡大などによって、新たな課題が発生すると考えられる。当社は、これらの課題解決に資する、IoTがもたらす未来の実現に必要な基盤技術の開発に引き続き取り組んでいく。

参 考 文 献

- http://www8.cao.go.jp/cstp/gaiyo/sip/keikaku/6_jidousoukou.pdf
- <http://www.mitsubishielectric.co.jp/building/automation/facima/solution/security/index.html>
- <http://www.mitsubishielectric.co.jp/news/2015/0721.pdf>
- <http://www.mitsubishielectric.co.jp/news/2015/0205.pdf>
- <http://www.mitsubishielectric.co.jp/news/2016/pdf/0217-f.pdf>
- <http://www.mitsubishielectric.co.jp/news/2016/0204.html>
- <http://www.mitsubishielectric.co.jp/news/2015/0128-a.html>
- <http://www.mitsubishielectric.co.jp/news/2014/pdf/0213-s09.pdf>
- 田村孝之、ほか：IoTプラットフォームのアーキテクチャ、三菱電機技報、90、No.7、383～387 (2016)
- 伊藤正裕、ほか：三菱電機スマート制御クラウドサービス“DIAPLANET”、三菱電機技報、89、No.8、430～433 (2015)

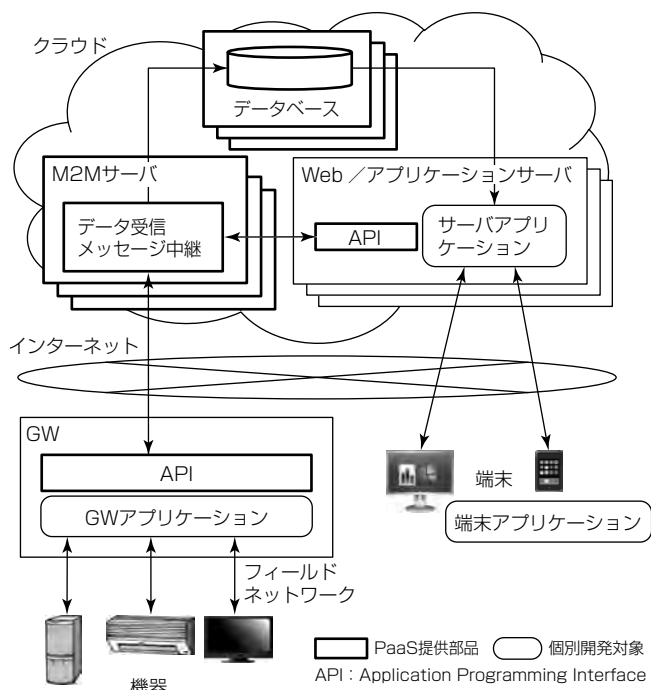


図3. IoTシステムの全体構成例

田村孝之* 渡邊和樹**
塚本良太**
原田篤史***

IoTプラットフォームのアーキテクチャ

Architecture of an IoT Platform

Takayuki Tamura, Ryota Tsukamoto, Atsushi Harada, Kazuki Watanabe

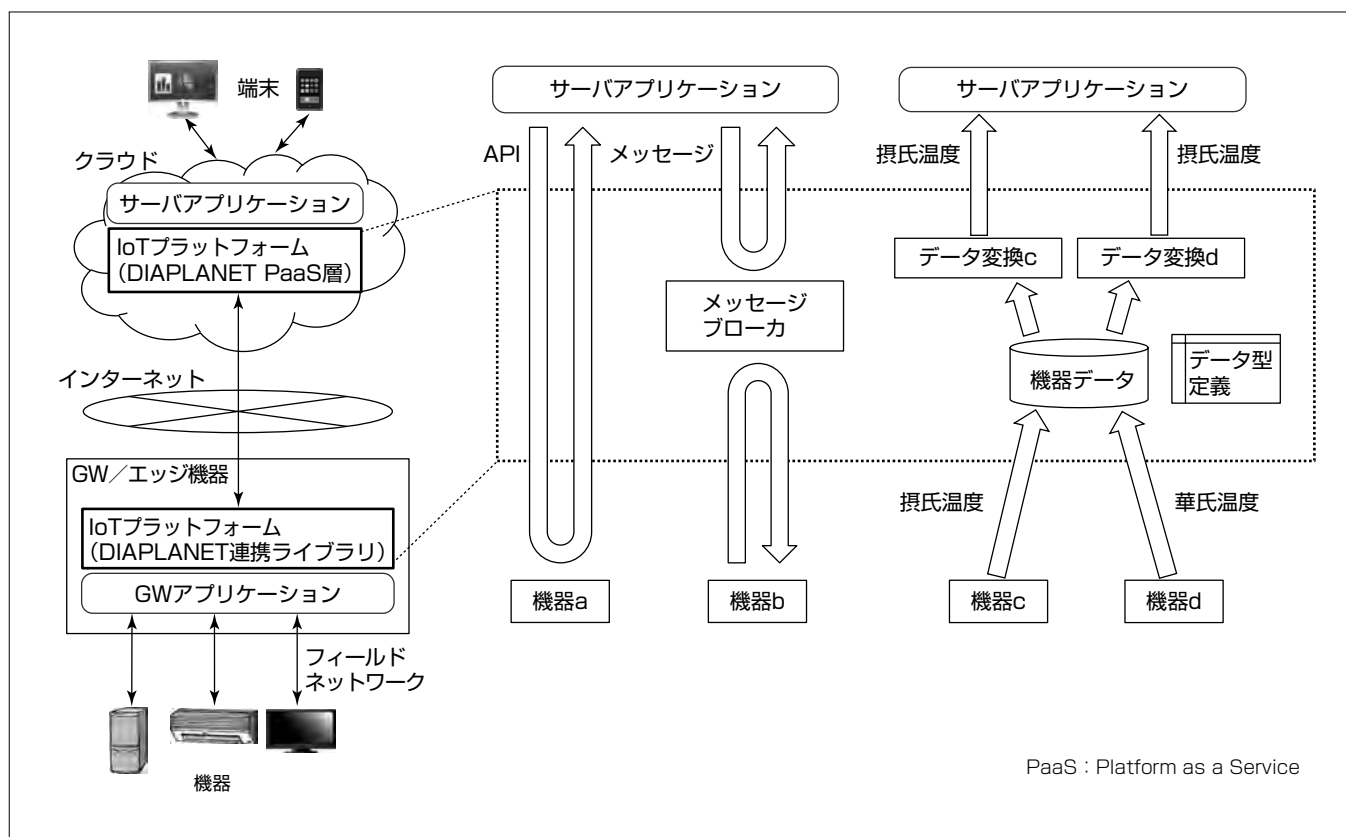
要 旨

様々なモノをネットワークに接続し、遠隔監視や遠隔制御等を実現するIoT(Internet of Things)が注目を集めている。三菱電機では、様々な機器に対するIoTアプリケーションの共通プラットフォームとして、スマート制御クラウドサービス“DIAPLANET”を提供している。

機器、ゲートウェイ(GW)/エッジ機器、クラウド、端末等からなるIoTシステムの構築を容易にするため、通信方式やデータ形式等の標準化が進められているが、多数の標準が併存しているのが実状である。そのため、IoTシステムでは、多様な通信方式を用いて機器とクラウドを接続し、多様な形式の機器データを管理することが求められる。また、機器データの分析手法は、実データから得られる知見に基づいて継続的に改良されるため、システム運用開始

後もデータ構造の変更等に柔軟に対応できることが望ましい。

DIAPLANETでは、クラウドと機器の通信における通信プロトコルと通信のパターンを隠蔽・変換するAPI(Application Programming Interface)を提供し、サーバアプリケーションの可搬性を高めた。また、機器データの管理では、機器から受け取った生データを標準形式のデータベースに格納しておき、サーバアプリケーションがデータを読み出す際に変換を施すことで、アプリケーションごとのデータベース設計を不要にした。これによって、データ収集開始までのリードタイム短縮と、アプリケーション仕様の継続的な変更を可能にした。今後は、クラウド及びエッジ機器でのデータ分析を支援する機能の充実化を図る。



IoTプラットフォームによる機器の多様性への対応

IoTプラットフォームは、クラウド上のサーバアプリケーションを様々な機器と連携可能にする。機器へのメッセージ送受信では、サーバ型の機器、クライアント型の機器に共通のAPIを提供する。機器データは標準形式のデータベースに格納し、サーバアプリケーションがデータをアクセスする際にデータ形式や解釈方法(例：温度の単位系)の変換を行う。

1. ま え が き

様々なモノをネットワークに接続し、遠隔監視や遠隔制御等を実現するIoTシステムでは、多様な機器を接続し、多様な機器データを扱うことが求められる。当社ではIoTシステムの開発・運用効率向上のため、機器接続と機器データ管理での多様性を吸収するIoTプラットフォームの開発を行っており、その成果を当社スマート制御クラウドサービスDIAPLANET⁽¹⁾に適用してきた。

本稿では、IoTシステムにおける多様性と、それに対処するためのIoTプラットフォームの機能について述べる。

2. IoTシステムの多様性

この章ではIoT標準の状況を概観し、IoTアプリケーションの開発では異なる標準の考慮が必要であることを述べる。特にIoTアプリケーションへの影響が大きい差異として、通信におけるメッセージ交換パターン、機器データの形式と解釈、機器の制御命令と制御結果について取り上げる。

2.1 IoT標準の状況

機器、ゲートウェイ(GW)、クラウド、端末等からなるIoTシステムの構築を容易にし、IoTアプリケーションの再利用性を高めるために、様々な標準が提案されている。図1は、IoT関連の主な標準やアライアンスのポジショニングを、適用レイヤ(垂直方向)及び適用フェーズ(水平方向)にマッピングしたものである。これらは、ネットワークレイヤの相互接続性に特化したものからアプリケーションレイヤにおけるエコシステム形成を意図したものまで多岐にわたっており、図1の全領域をカバーする単一の標準に収束する見込みは低いと考えられる。

例えばネットワークレイヤでは、機器/GWとクラウド間の通信に用いられるプロトコルとしてHTTP, CoAP, MQTTなどがあり、複数プロトコルの混在を許してシス

テム構成の自由度を高めることが望ましい。そこで、標準に対応しつつ個々の標準の差異を隠蔽するIoTプラットフォームによって、複数の標準に対応したIoTアプリケーションの開発を効率化する必要がある。

2.2 メッセージ交換パターン

IoT標準ごとに大きく異なるものの1つに、機器とアプリケーション間のメッセージ交換パターンがある。図2に機器からのデータ収集における主なメッセージ交換パターンを示す。

図2(a)は機器がサーバ機能を持ち、アプリケーションの要求を受け付けて応答するものである。アプリケーションは任意のタイミングで機器に最新の状態を問い合わせ、応答に基づいて画面更新等を行う。工場や設備内のローカルネットワーク上でパソコン等を用いた管理や見える化が可能な機器やアプリケーションはこのパターンに対応している。機器とアプリケーションをインターネット経由で接続する場合は、機器のサーバ機能を第三者に公開することを防ぐため、VPNルータを用いることが多い。しかし、アプリケーション側から工場・設備内ネットワーク上の機器が全てアクセス可能となってしまうため、セキュリティ確保のためには精緻なアクセス制御が必要である。

図2(b)は機器がクライアントとなって自律的に状態を通知するものであり、MQTT等のプロトコルが適用される。アプリケーションは機器が通知する状態データを直接受信するのではなく、一旦データベースに格納されたデータを用いて見える化等を行うことが多い。機器が設置される環境はNATルータを介してインターネット接続されることが多いが、機器をサーバとして公開する必要のないこのパターンはこのような環境と親和性が高い。

図2(c)は両者の中間であり、サーバ機能を持つ機器がアプリケーションからの要求をトリガーとし、指定された周期で持続的に状態データを応答するものである。

異なるメッセージ交換パターンの間でアプリケーションを再利用するには、メッセージ交換パターンを変換する機能の追加が必要になる。例えば、通知型のアプリケーションを要求・応答型の機器と組み合わせるには、応答データをデータベースに格納する別アプリケーションを追加する。一方、要求・応答型のアプリケーションを通知型の機器と組み合わせるに

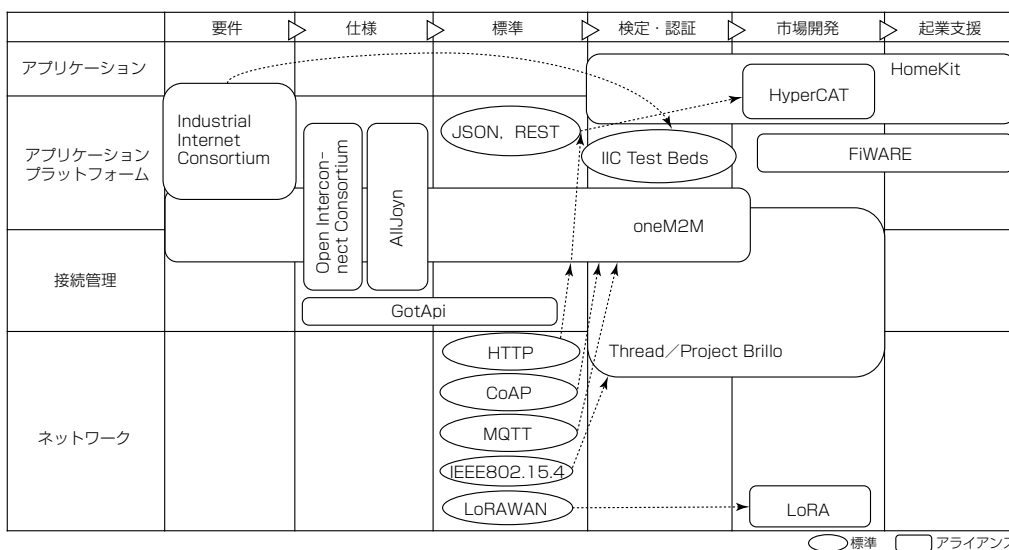


図1. IoT関連標準とアライアンスのポジショニング⁽²⁾

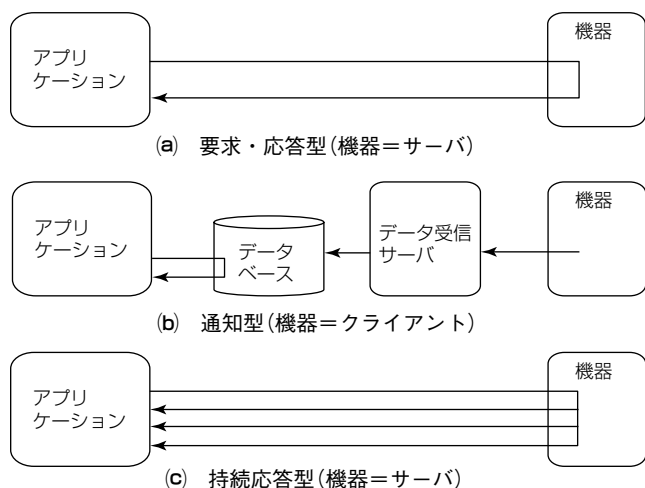


図2. 機器データ収集におけるメッセージ交換パターン

は、機器への要求をデータベースへの問合せに変換する処理が必要になる。IoTプラットフォームによってこれらの変換を行うことで、アプリケーションの再利用性を高めることができる。

2.3 データ形式と解釈

標準や機器ごとにデータの表現方法にも差異が生じる。これにはXML(eXtensible Markup Language)やバイナリなどの、エンコーディング形式の違いも含まれるが、より重大な差異は、値の解釈に関するものである。

例えば温度では摂氏及び華氏のどちらの単位系で表されるかによって同じ物理量に対応する数値が異なってくる。また、電力量では、ある機器は30分ごとの積算値を出力し、別の機器は計測開始以降の積算値を出力するというように、値の定義に含まれるパラメータ(この場合は積算対象の時区間)が異なる場合がある。さらに、センサの生データのように、読み取った値から元の物理量を求めるのに補正処理が必要になる場合もある。

値の解釈に必要な単位系や補正パラメータ等の情報は、機器・センサの仕様や設置条件としてオフラインで与えられることが多い。したがってIoTアプリケーションがこれらの値を解釈するロジックを内蔵してしまうと、仕様や設置条件が異なる同種の機器への適用が困難になる。そこで、データの値にその解釈方法を示す情報を明示的に付与し、IoTプラットフォームに値の解釈を行うロジックをライブラリとして持たせることで、IoTアプリケーションの汎用性を高めることができる。

2.4 制御命令と制御結果

アプリケーションから機器に命令を送付して制御を行う場合、機器ごとに命令の内容が異なることに加え、制御結果の応答内容が持つ意味にも差異が生じる。すなわち、応答内容が制御命令実行後の機器の状態を反映する場合と、単に制御命令の受領を示すに過ぎない場合である。後者の場合、制御命令がいつ有効になったかを確認するために、

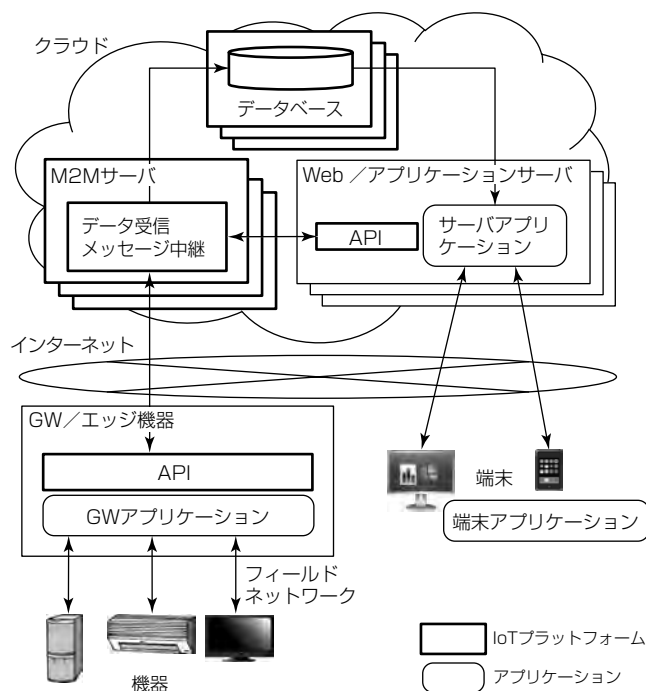


図3. IoTシステムの全体構成例

機器の状態を取得する命令を別途発行する必要がある。

状態問合せの結果についても、ハードウェアの現在の状態を返す機器と、キャッシュされた過去の状態を返す機器が存在する。レガシー機器にハードウェアを外付けしてスマート化した機器では、操作パネルやスイッチ等で本体を直接制御すると外付けハードウェア側ではその内容を検知できない。このような外付けハードウェアが状態をキャッシュする方式を採用していると、機器本体の状態との一貫性を維持できなくなる。

IoTプラットフォームは、制御命令に単なる受領確認で応答する機器に対し、状態が変化するまで問合せを行うことで、各アプリケーションの処理を単純化することができる。

3. IoTプラットフォームの構成

この章では2章で示したIoTシステムの多様性に対応するためのIoTプラットフォームの構成について述べる。はじめにIoTシステムの全体構成におけるIoTプラットフォームの位置付けを示し、機器とのメッセージ交換パターンの差異を吸収する方式、及び機器データの解釈の差異に対応するデータベース設計について述べる。

3.1 全体構成

図3にIoTシステムの全体構成例を示す⁽¹⁾。IoTシステムは機器、GW/エッジ機器、クラウド、及び端末からなり、IoTプラットフォームはクラウド上のサーバアプリケーション及びGW/エッジ機器上のGWアプリケーションに対してAPIを提供する。GW/エッジ機器の機能を機器に組み込み、機器が直接クラウドと通信する構成も取り得る。

M2M(Machine to Machine)サーバは、サーバアプリケーションが機器データを利用するための基本機能として、クラウド上でGW／エッジ機器からデータを受信し、データベースに格納する機能を提供する(図2(b)のデータ受信サーバ)。また、M2Mサーバは、サーバアプリケーションから機器に対して要求を送信するための基本機能として、クライアント型のGW／エッジ機器とWeb／アプリケーションサーバの双方向通信を可能にするメッセージ中継(ブローカ)機能を提供する。

データベースはKVS(Key-Value Store)であり、アプリケーションの要件に応じて関係データベース(Relational DataBase：RDB)を併用する。データベースでは、任意の機器データをデータ型名とともに記録することで、データ変換等の処理の詳細を柔軟に変更可能とする。また、KVSはキー値に基づく分散管理が容易であり、サーバを追加してスケールアウトすることでデータ量の増大に対応することができる。

接続するGW／エッジ機器数や端末数の増加に対しては、M2MサーバやWeb／アプリケーションサーバの追加によるスケールアウトで対応する。IoTプラットフォームのクラウド側構成要素は仮想サーバイメージで提供され、クラウド管理機能によってインスタンス数を制御することで最適なシステム構成を維持する。スケールアウト構成とすることで、GW／エッジ機器と接続するM2Mサーバと、端末と接続するWeb／アプリケーションサーバがアクセスの都度異なる可能性が生じるが、両者を中継するメッセージ中継機能を通信相手のアドレスを直接指定しないPub／Sub通信に基づいて実現することでこれに対応している。

端末とWeb／アプリケーションサーバの接続部分、及びGW／エッジ機器とM2Mサーバの接続部分では、それぞれユーザー認証及び機器認証を行う。GW／エッジ機器に対しては、クラウドへの初期登録機能、クラウドからの証明書配布・証明書更新機能が必要になる。

次にIoTプラットフォームの主要な構成要素について述べる。

3.2 メッセージ通信API

3.1節で述べたIoTプラットフォームでは、多様な機器に対するアプリケーションの独立性を高めるため、異なる通信プロトコルやメッセージ交換パターンに対し、共通のAPIを提供する。図4にメッセージ通信APIの外部インタフェースの1つと内部動作例を示す。

サーバアプリケーションがGW／エッジ機器にメッセージを送信する際は、送信先のGW／エッジ機器ID(“devA”)とメッセージ内容(“msg”)を指定してAPIを呼び出す(Request-Response)。API実装の内部ではMQTT等のPub／Sub型通信を用い、M2Mサーバのメッセージ中継機能であるPub／Subブローカに対してこれらの情報をPublish(出版)する。この際、応答メッセージを受信す

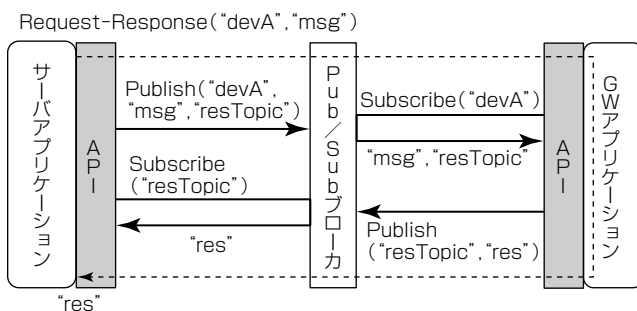


図4. メッセージ通信APIと内部動作

るための論理的なアドレスであるトピックを動的に生成し(“resTopic”), メッセージ内容に付与する。

GWアプリケーションは自身のGW／エッジ機器IDをトピックとしてAPI経由でPub／SubブローカにSubscribe(購読)要求を発行しておき、このIDに対してメッセージが発行されると瞬時にその内容と応答用トピックを受け取る。GWアプリケーションは受信したメッセージに従って機器の制御や状態取得を行い、応答メッセージ(“res”)を生成すると、APIを介して応答トピックに対して応答メッセージをPublishする。

サーバアプリケーションはメッセージのPublishと並行して、応答トピックに対するSubscribeを行い、GW／エッジ機器から応答メッセージがPublishされると瞬時にそれを受信する。

このように、APIはGW／エッジ機器側がクライアントとなる通信プロトコルを用いて、要求・応答型のメッセージ交換パターンを提供しており、GW／エッジ機器側をサーバと想定して実装されたアプリケーションの移植を容易にする。他の通信プロトコルを用いる場合でも、実装詳細は隠蔽可能であり、APIを共通に保つことができる。

GW／エッジ機器の台数増加に対しては、Pub／Subブローカを複数用意し、負荷分散を行うことで対応する。同時に、Pub／Subブローカの障害への耐性を得るため、複数ブローカへの同報を行う。こうしたクラスタリング機能をPub／Subブローカ自体が備えていることもあるが、API実装内部で実現することでその他のブローカも利用可能としている。これらによって、共通APIを維持したままスケールアウトを実現できる。

アプリケーションの移植性を高めるだけでなく、アプリケーション自体の再利用が求められる場合もある。このような場合は、サーバやGW／エッジ機器で通信エージェントソフトウェアを動作させ、通信プロトコル及びメッセージ交換パターンの変換を行う。図5はGW／エッジ機器上の通信エージェントによって、Pub／Sub型の通信プロトコルで受信したサーバアプリケーションからのメッセージを、HTTP等の要求・応答型の通信に変換して既存のGWアプリケーションに受け渡す例である。

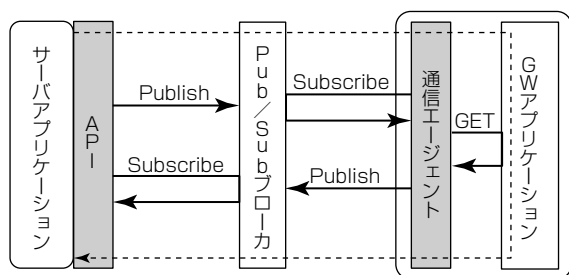


図5. 通信エージェントによる通信方式の変換

同様に、クラウド側に通信エージェントを置き、要求・応答型の通信をPub/Sub型に変換することもできる。HTTPを用いるサーバアプリケーションに対しては、通信エージェントはプロキシサーバとして振る舞う。

3.3 データベース

M2Mサーバのデータ受信機能がデータを格納するデータベースはKVSをデフォルトとし、任意形式のデータをタイムスタンプ、センサ等データソースのID、データ型名とともに記録する構造を標準としている。RDBに基づくシステム開発のようにアプリケーションごとに最適なスキーマを事前に定義する開発手順では、機器データ収集開始までのリードタイムが大きくなってしまふ。また、収集したデータから得られた知見に基づくアプリケーション改良に伴ってスキーマを変更する際は、蓄積したデータのマイグレーション処理が必要となる。データの形式と解釈に必要な情報をデータ型名として記録しておくことで、任意のデータを単一の構造で扱うことが可能となり、事前のスキーマ定義が不要となる。また、アプリケーションの要件が変わった際には、データ変換等の処理の詳細を柔軟に変更することができる。

自己記述的なデータによってデータの構造と解釈を疎結合にするアプローチは、“Late-bound schema” “Schema-on-Read”などと称され、IoTシステムにおけるビッグデータ管理に適した手法とみなされている⁽³⁾。また、こうしたアプローチに基づいて多種多様なデータを生のまま集積したりポジトリは、企業内データにおけるデータウェアハウスと比してデータレイクと呼ばれる⁽⁴⁾。

一方、同一データに繰り返しアクセスし、対話的な応答が求められる可視化アプリケーション等に対しては、データの解釈を読み出し時に決定するこのアプローチでは十分な速度性能が得られない場合がある。そこで、KVSとともにRDBを併用し、定型的なデータ変換の結果をRDBに格納してアプリケーションからアクセスするようにする。RDBへのデータ格納は、KVSからETL(Extract-Transform-Load)ミドルウェアを用いる方法と、M2Mサーバのデータ受信機能のカスタマイズによってKVSへの格納と並行して行う方法を選択できる。ETLを用いる方法は、データ受信に影響を与えずにRDBのスキーマを

変更できるため、より一般的である。

データにデータ型名を付随させるアプローチでは、データ型名とデータ処理方法を1対1に対応付ける必要がある。データ型名の衝突や別名の発生を避けるため、命名規則の整備が課題である。ベースとしては、Webやメール等のインターネットアプリケーションで様々なコンテンツ形式の表現に用いられるMIMEタイプが利用できるであろう。データ型名と対応付けてデータ変換のロジックを集積し、ライブラリ化していく。また、機器のファームウェアを更新した際は、機器データの仕様が変更され得る。このような場合、データ型名も合わせて変更することが望ましいが、GW/エッジ機器側で対応できない場合もある。そのため、データ型名自体のバージョン管理を行い、データのタイムスタンプと組み合わせでデータ変換ロジックの選択を行うようにする。機器側の構成管理との連携が重要になると考えられる。

4. む す び

IoTシステムの多様性に対応し、IoTアプリケーションの開発を効率化するためのIoTプラットフォームの機能について述べた。クラウドと機器の間の通信に対しては、使用プロトコルとともにメッセージ交換のパターンを隠蔽・変換するAPIを提供することでアプリケーションの可搬性を高めた。また、機器から受け取ったデータを共通データ構造に一旦格納し、読み出す際にアプリケーションの要件に従った変換を施すことで、多様な機器データの柔軟な管理を可能にした。

今後、IoTプラットフォームでは、データ分析を支援する機能の充実化を進める。特に、クラウドとエッジ機器の連携による効率的かつセキュアなデータ分析の実現について検討していく。

参 考 文 献

- (1) 伊藤正裕, ほか: 三菱電機スマート制御クラウドサービス“DIAPLANET”, 三菱電機技報, **89**, No.8, 430~433 (2015)
- (2) Fiqueredo, K.: IoT alliances and interoperability (2015)
<http://www.more-with-mobile.com/2015/06/iot-alliances-and-interoperability.html>
- (3) Abadi, D., et al.: The Beckman Report on Database Research, CACM, **59**, No.2, 92~99 (2016)
- (4) Dixon, J.: Pentaho, Hadoop, and Data Lakes (2010)
<https://jamesdixon.wordpress.com/2010/10/14/pentaho-hadoop-and-data-lakes/>

海外におけるEMSソリューション

滝田大介* 大塚 晃*
京屋貴則*
飯島昌平*

EMS Solutions in Overseas Market

Daisuke Takita, Takanori Kyoya, Shohei Iijima, Akira Otsuka

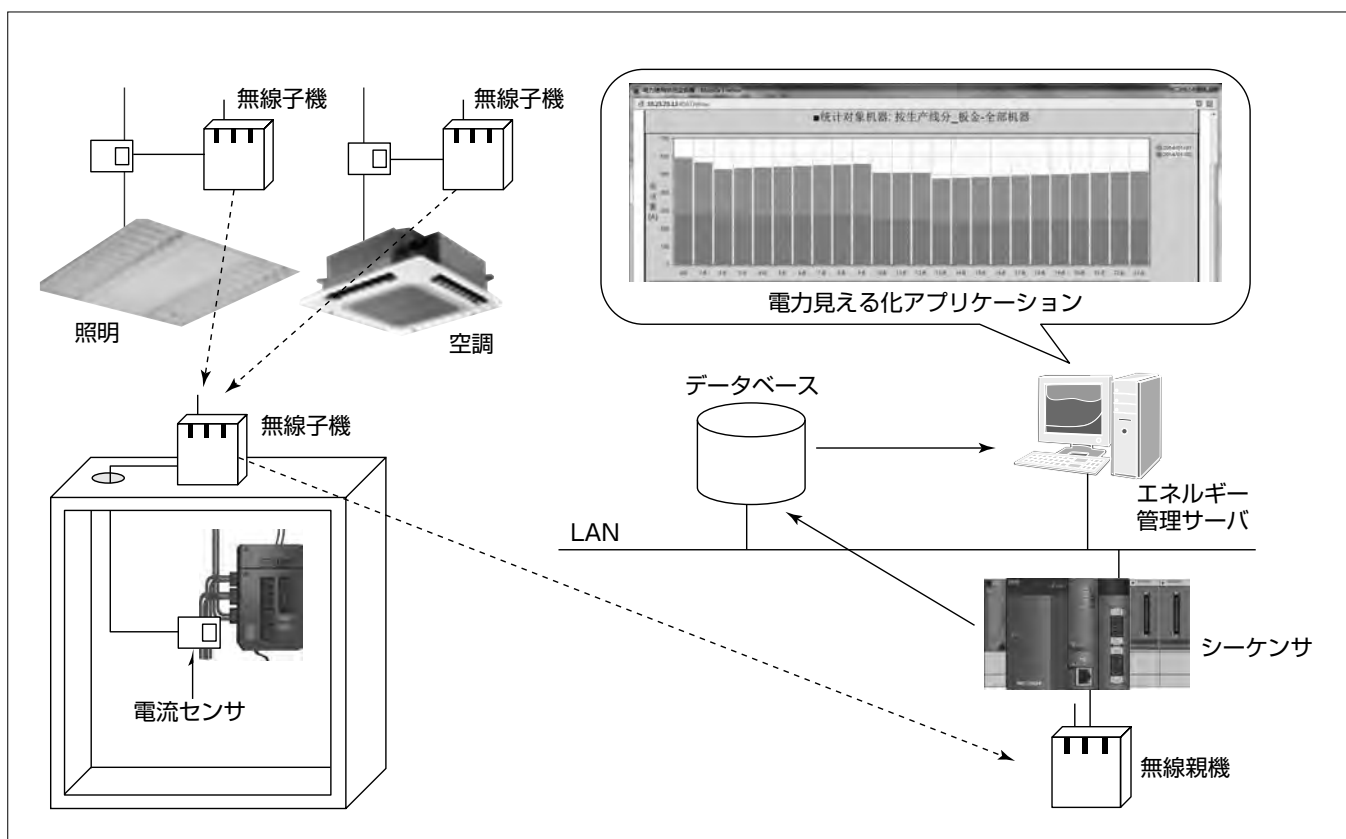
要 旨

中国やASEAN(東南アジア諸国連合)地域など成長著しいアジアの新興国で、急速な経済成長に伴い、電力不足、コスト削減、環境規制への対応など、様々な要因からエネルギー消費量の削減が課題となっている。

三菱電機は国内外関連会社と連携し、これらの新興国で、エネルギー消費量の可視化を中心とした省エネルギーを推進するエネルギーマネジメントシステム(Energy Management System:EMS)を、各国の法規制やニーズ、ビル・工場といった使用条件に合わせたソリューションとして提案し、省エネルギー効果の確認やデータ取得を目的とした実証実験を行っている。このEMSソリューションは、

サブギガヘルツ帯無線通信による設置工事の簡易化、自律分散的なネットワーク構築技術による拡張性、及び、視覚的にデータを表示するアプリケーションを組み合わせることを特長としている。このため、低コストかつ短期間でのカスタマイズが可能であり、実証実験や分析結果に基づく構成変更を容易に行うことができる。

今後、この実証実験によって得られたデータ・知見を活用して、様々な顧客が抱える本質的な課題を明確にし、より効果的なソリューションを提案することによって、事業機会の獲得や、既存事業の競争力強化につなげていく。



工場のEMSソリューション

設置工事が容易な無線通信機に接続された電流センサを多数設置し、自律分散的なルーティングアルゴリズムによって無線ネットワークを自動構築する。無線ネットワークを介して収集したセンサ情報を、既設のLAN上に設置されたデータベースに蓄積し、エネルギー管理サーバ上のアプリケーションによって、エネルギー使用のきめ細かい見える化を実現する。

1. ま え が き

中国やASEAN地域など成長著しいアジアの新興国で、急速な経済成長に伴い、電力不足、コスト削減、環境規制への対応など、様々な要因からエネルギー消費量の削減が課題となっている。

当社は国内外関連会社と連携し、これらの新興国で、エネルギー消費量の可視化を中心とした省エネルギーを推進するEMSを、各国の法規制やニーズ、ビル・工場といった使用条件に合わせたソリューションとして提案し、省エネルギー効果の確認やデータ取得を目的とした実証実験を行っている。このEMSソリューションは、サブギガヘルツ帯無線通信による設置工事の簡易化、自律分散的なネットワーク構築技術による拡張性、及び、データ分析を容易にするアプリケーションを組み合わせることを特長としている。このため、低コストかつ短期間でのカスタマイズが可能であり、実証実験や分析結果に基づく構成変更を容易に行うことができる。

2. 海外向けEMS

急速な経済成長に電力供給が追いつかず電力不足に悩まされている地域、人件費の上昇など事業環境の変化のためにコスト削減に迫られる企業、環境問題の顕在化への対応の一環としてCO₂排出規制を強化する政府など、様々な方面からの動機付けによって、アジア新興国における省エネルギーに対する関心が少しずつ高まり始めている。

省エネルギーに取り組むに当たり、現状の把握と分析は最も重要なプロセスである⁽¹⁾。ビル・工場といった使用条件に加え、気候や風土などの自然条件、法規制や商習慣、価値観などの文化的条件、電力コストや電力供給状況などが大きく異なるため、エネルギーの消費スタイル及び省エネルギーのために求められるソリューションも千差万別である。そこで、導入容易性を特長とした、エネルギー消費状況の現状把握と分析を可能とするEMSを開発し、様々な条件下での実証実験を実施している。はじめに敷居の低いこのEMSを導入し、これによって得たデータと知見を活用しながら、その後の協力関係の継続や、協業分野の拡大につなげることを主な狙いとしている。

3. 要素技術

3.1 無線ネットワーク技術

このEMSでの無線ネットワークの通信プロトコルスタックを表1に示す。モノとモノとの通信(Machine to Machine：M2M)におけるセンサネットワークに要求される、低消費電力及び通信範囲拡大を可能とする機能構成⁽²⁾としている。

表1. 無線ネットワークの通信プロトコルスタック

レイヤ	方式名
物理層	IEEE 802.15.4g ⁽⁴⁾
物理媒体	各国法令に準拠
通信速度	100kbps
データリンク層	IEEE 802.15.4 ⁽³⁾
メディアアクセス制御	CSMA/CA
ネットワーク層	独自方式
経路制御	RPL ⁽⁶⁾ ベースの独自方式
アプリケーション層	独自方式

CSMA/CA：Carrier Sense Multiple Access with Collision Avoidance

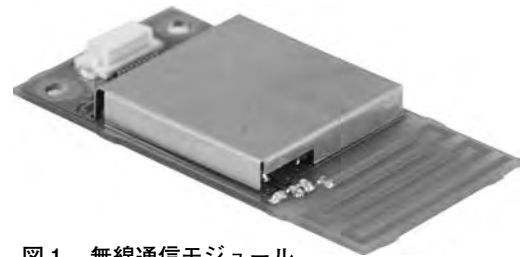


図1. 無線通信モジュール

3.1.1 無線通信方式

IEEE802.15.4⁽³⁾は、デバイスの低消費電力化が容易となるように方式設計された無線通信規格である。これに加えて、サブギガヘルツ帯を使用する仕様を追加した拡張規格IEEE802.15.4g⁽⁴⁾を物理層に採用している。サブギガヘルツ帯は、電波到達性、回折性に優れ、2.4GHz帯などと比較して電波干渉が少ない点を特長とする。日本ではスマートメータ等に用いられる920MHz帯特定小電力無線が代表的なサブギガヘルツ帯の規格であるが、各国によって使用可能な周波数は異なる。このEMSでは920MHz帯特定小電力向けに開発した無線通信モジュール⁽⁵⁾(図1)を各国法令に準拠するように拡張開発し、センサネットワークの構築に使用した。

3.1.2 ネットワーク方式

RPL⁽⁶⁾(Routing Protocol for Low-power and lossy networks)をベースとした独自の経路制御プロトコルを実装し、複数の冗長経路を使用可能なマルチホップ無線通信(メッシュネットワーク)を実現した。これによって、マルチホップ通信によるデータ収集範囲の拡大、冗長経路設定による障害の回避、自律分散制御による経路設定の自動化など、管理コストの削減が可能となる。RPLはIPv6(Internet Protocol version 6)ネットワークを想定した経路制御プロトコルであるが、このEMSではnon-IPで動作するRPLを開発し、ソフトウェアの軽量化を図った。

図2にRPLによる経路構築の流れを示す。

はじめに、ルートノードとなる無線親機が、DIOメッセージをブロードキャスト送信する。このとき、DIOに含まれるランクと呼ばれる情報要素を0に設定する。各無線子機は、受信した複数のDIOのランクのうち、最小のものに1を足した値を自身のランクとし、自身のランク値を持

つDIOをブロードキャスト送信する。このとき、受信したDIOのうち、自身のランク値よりも小さいランク値を持つものの送信元を上り経路の次ホップとして経路表に保持する。全無線子機がこれを繰り返すことによって、各無線子機から無線親機に到達するための上り経路が設定される(図2(2))。

この後、各ノードは上り経路の次ホップに対してDAOメッセージを送信する。DAO中のターゲットアドレスを自身のIDとする。DAOを受信したノードは、そのターゲットアドレス宛の下り経路の次ホップが、DAOの送信元であることを経路表に記録し、そのターゲットアドレスを含むDAOを自身の上り経路の次ホップに転送する。この繰り返しによってDAOは無線親機に到達し、無線親機

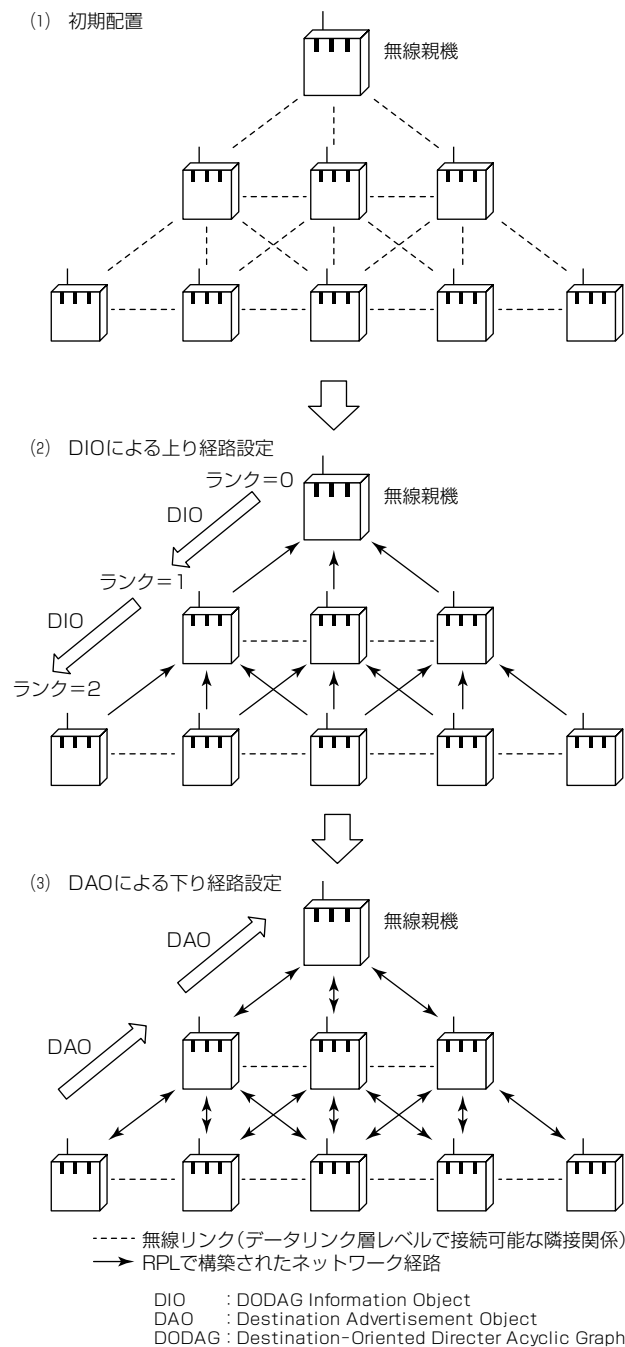


図2. RPLによる経路構築の流れ

から各無線子機にいたる下り経路が設定される(図2(3))。

3.2 アプリケーション

EMSソリューションで用いられるアプリケーションに求められる基本的な機能は、電力量等のデータを適切な精度で“見える化”することである。潜在的なエネルギー消費の無駄を明らかにすることで、省エネルギー対策の具体化がより容易となる。例えば、工場の製造設備や空調、照明が消費する電力量を1時間ごとの精度で“見える化”することで、生産に寄与しない時間帯の“削減可能な消費電力”や、生産設備が発生する熱による“空調への追加負荷となる消費電力”を掌握できるようになる。更なる消費電力の削減には、生産計画の変更による“電力消費の平準化”や“稼働時間帯のシフト”“集中稼働による消費電力の効率化”等の手法が有効であるが、生産性やコスト、品質への影響、人員計画との連携といった省エネルギー以外の要素を考慮することが必要である。

無線ネットワークを介して収集する各種データを“見える化”するアプリケーションのシステム構成を図3に示す。このEMS構成では、電力測定の対象となる機器の動力線に電力量をセンスするCTを設置し、無線ネットワークでシーケンサに送信したデータをMES(Manufacturing Execution System)インタフェースユニットを介してデータベースに蓄積する。データベースには、省エネルギー対策に必要な温度、湿度、照度等のデータも保存される。比較したいデータを加工し、1時間ごとの精度で“見える化”する。

3.3 支援ツール

無線システムの構築では、設計・設置・保守の3段階で、電波到達範囲や雑音環境を考慮した無線機の設置場所の決定、設置後の通信確認や状態監視、異常検出や障害からの復旧などの作業が必要である。そこで、無線通信の専門知識を持たないユーザーでもこれらの作業ができるように、直感的なユーザーインタフェースを備えた各種の支援ツールを開発

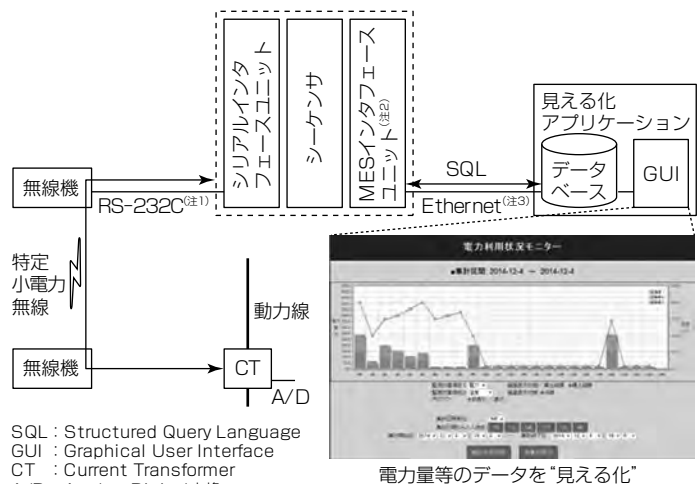


図3. 見える化アプリケーション

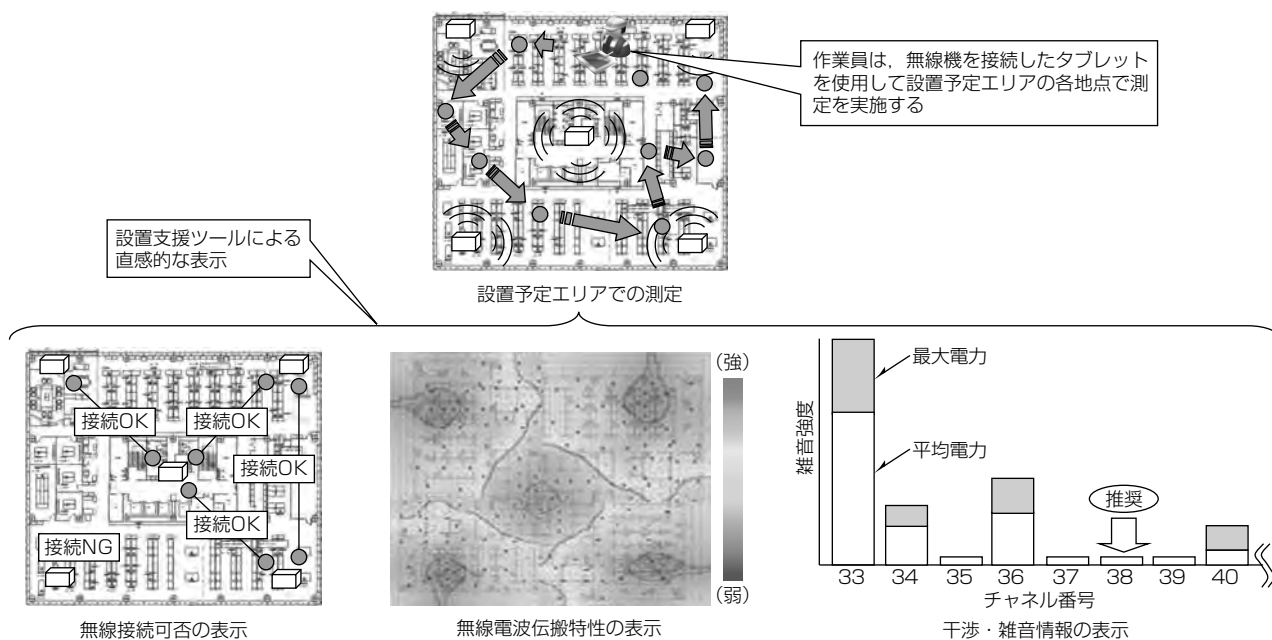


図4. 設置支援ツールのイメージ

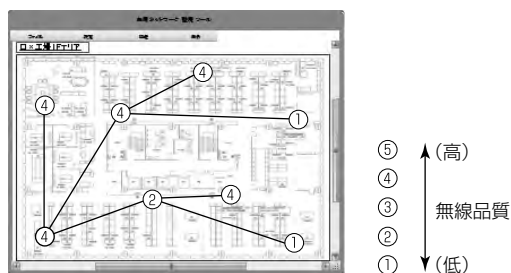


図5. 無線ネットワーク監視ツールのイメージ

表2. 実施中の実証実験

実証実験場所	目的
工場(中国)	無線伝搬調査, 運転コストの削減
ビル(中国)	無線伝搬調査, デモンストレーション
商業施設(中国)	空調の効率化
ビル(シンガポール)	熱帯地域における電力消費の実態調査

した。代表的な支援ツールのイメージを図4及び図5に示す。

図4に示す設置支援ツールは、作業員による受信電力測定結果に基づき、無線接続可否、無線電波伝搬特性、干渉・雑音情報などを表示することができる。また、図5に示す無線ネットワーク監視ツールは、無線ネットワークの接続状態を可視化し、保守をサポートする。

4. 海外での実証実験

先に述べた各種の技術を組み合わせ、海外で実証実験を実施している。現在実施中の実証実験を表2に示す。これまでの実証実験の結果、迅速な要件抽出や実験的試行の繰り返し等、このEMSのメリットが各国のニーズに合致することが分かった。エネルギーコストの削減効果も含めたコストメリットを明らかにし、事業モデルを構築することが今後の課題である。

5. む す び

無線技術の応用と各種の可視化ツールを組み合わせることによって、低コストかつ短期間でのカスタマイズが可能なEMSソリューション、及び、海外における実証実験について述べた。

今後、これらの実証実験によって得られたデータ・知見を活用して、様々な地域の様々な顧客が抱える本質的な課題を明確にし、より効果的なソリューションを提案することによって、事業機会の獲得や、既存事業の競争力強化につなげていく。

参 考 文 献

- (1) 三菱電機省エネサポートサイト
<http://www.mitsubishielectric.co.jp/shoene/>
- (2) 藤江良一, ほか: M2Mを支える無線/ネットワーク技術, 電子情報通信学会 総合大会BT-3-1 (2013)
- (3) IEEE Std 802.15.4, Part 15.4: Low-Rate Wireless Personal Area Networks(LR-WPANs) (2011)
- (4) IEEE Std 802.15.4g, Part 15.4: Low-Rate Wireless Personal Area Networks(LR-WPANs), Amendment 3: Physical Layer(PHY) Specifications for Low-Data-Rate, Wireless, Smart Metering Utility Networks (2012)
- (5) 特定小電力無線を用いたセンサネットワーク, 三菱電機技報, 89, No.1, 7 (2015)
- (6) Winter, T., et al.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, IETF RFC6550 (2012)

イベント向け警備支援のための映像解析技術

宮城惇矢* 古木一朗*

西辻 崇*

服部亮史*

Visual Analysis Techniques for Event Security Management

Junya Miyagi, Takashi Nishitsuji, Ryoji Hattori, Ichiro Furuki

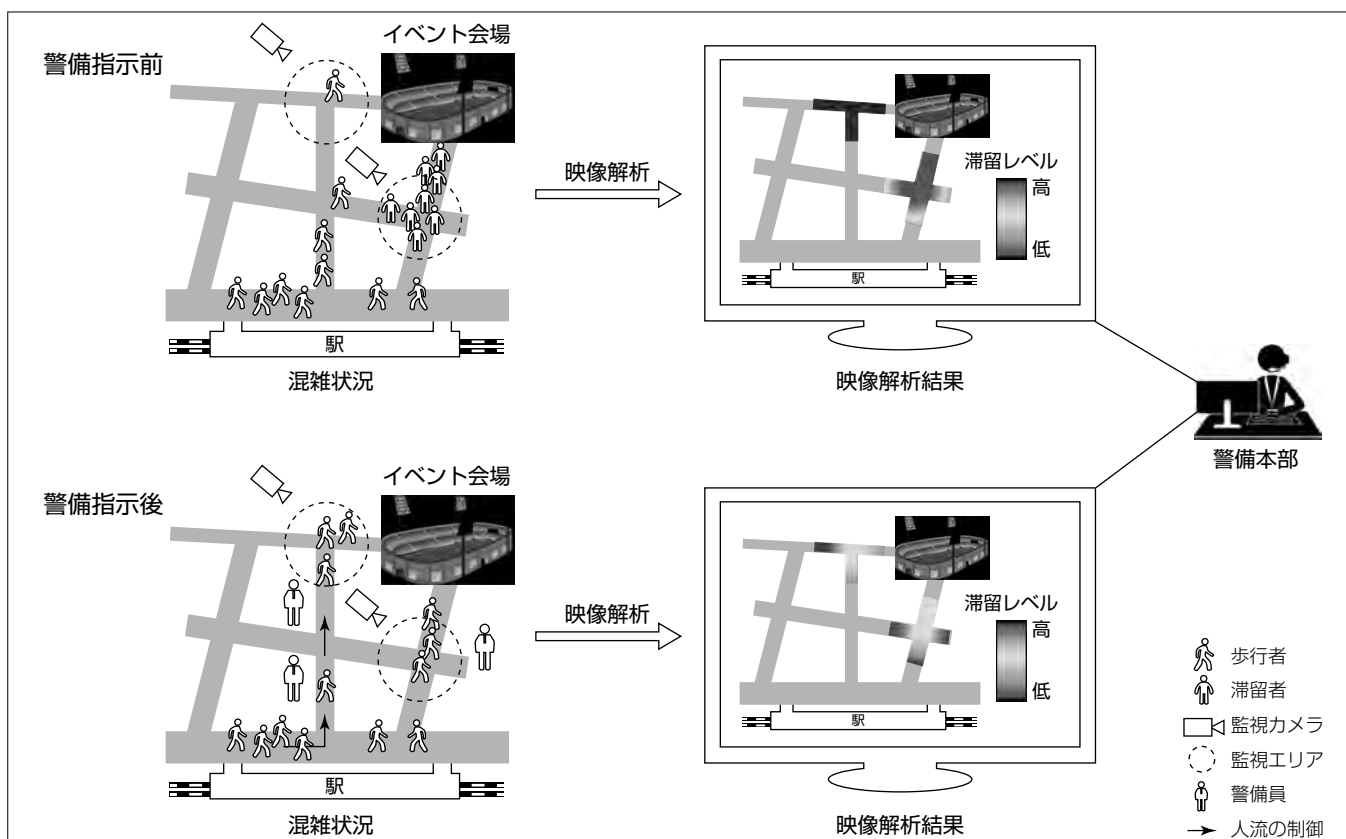
要 旨

花火大会やスポーツ大会等の大規模イベントでは、多数の参加者による群集雪崩のような雑踏事故発生の可能性がある。雑踏警備による混雑発生の早期発見と抑制が必要である。従来の雑踏警備では、現場の警備員からの主観的な情報を収集して判断するため、状況判断、警備指示は警備員の経験に大きく依存し、大規模イベントでは、適切な警備が困難になっている。三菱電機では、監視カメラ映像の解析と可視化によって、雑踏警備をITで支援する技術開発を進めている。映像解析によって混雑状況を数値化し、地図上で可視化して提供することで、混雑状況の判断・予測、それに基づく適切な警備指示を可能にする。

カメラ映像の解析技術として、ある区間の通過人数を推定する人流解析方式と、群集が移動できず滞留状態にあ

ることを検知する滞留検知方式を提案する。群集映像を用いて評価した結果、前者で人流誤差9%，後者で滞留状態検知正解率93%が得られ、適切に混雑状態を判断する可能性を確認した。両方式とも、低演算量が特長であり、監視カメラ内のプロセッサで十分に処理可能である。映像解析をサーバで実施する方式に比べ、解析のための映像伝送が不要で、データ量の小さい解析結果のみを伝送することができ、大規模イベント警備のための無線通信を用いた一時的なシステムも容易に構築可能である。

今後、既に開発したマルチホップ無線技術、俯瞰(ふかん)映像合成技術等と組み合わせ、雑踏警備のIT支援を進めていく。



警備支援に向けた映像解析技術の活用例

駅からイベント会場までの経路に監視カメラを設置し、監視カメラ映像を解析することで主として群集の動きに関する情報を用いて、混雑状況の可視化を行っている。図は地図上にヒートマップとして混雑状況を可視化したものである。警備本部では混雑状況をリアルタイムかつ正確に把握でき、適切な警備指示を速やかに出すことが可能になる。

1. ま え が き

花火大会やスポーツ大会、コンサート等のイベントでは、参加者の集中による混雑が発生する。イベントの大規模化に伴い、混雑は人命に関わる群集雪崩のような事故リスクの高い雑踏に変化するため、混雑の早期発見とその抑制を担う雑踏警備は重要である。

従来の雑踏警備では、イベント現場に配置された警備員の目視による混雑状況を、主観的・定性的な情報として警備本部に音声で伝達する。警備本部の警備員は、これらの情報を用い経験に基づき混雑状況を判断・予測して警備方針を決定するため、警備業務の質は警備員、特に本部警備員のスキルに大きく依存する。大規模なイベントでは、警備員の増加によって本部に伝達される情報が増え、警備エリア全体の正確な状況把握と適切な警備方針を決定することが困難となる。

この問題に対し、当社は映像解析に基づく混雑状態分析とその可視化によって、雑踏警備をITで支援する技術開発を進めている。イベント現場に設置した監視カメラの映像から混雑状態を数値化し、警備本部に地図上で混雑状況を可視化し提供することで、警備エリア全体の混雑状況把握精度の向上や適切な警備方針の決定を可能にする。このような適切な人流誘導によって雑踏事故リスクを低減し、安全・安心で快適なイベント実現に貢献する。

2章では混雑状態解析と可視化に基づくイベント警備支援システムの全体像、3章では監視カメラ映像による混雑状態解析技術について述べ、4章でまとめと今後の課題について述べる。

2. 混雑状態解析に基づくイベント警備支援

雑踏事故のリスクが高く、警備・誘導の重要性が高いイベントとして、公共交通機関を利用する花火大会やスポーツ大会、コンサート等の大規模イベントを想定する。駅とイベント会場間では、イベント参加者と一般通行者が交錯し、特にイベント終了後には、帰宅者が集中して混雑が発生するケースが多い。参加者は経路についての知識が乏しい場合も多く、前後にしか進めない道路上では退避行動がとれず、雑踏事故のリスクが増大する。

このようなイベントでは、経路上に多数配置される警備員からの定性的な報告よりも、道路上で双方向に移動する人数とその時間変化の把握、及び、移動する人数が減少したのか、混雑によって移動できずに滞留しているのかを監視カメラ映像から解析し、全体把握を行うことが重要である。

監視カメラは、防犯用途又は事件・事故の要因分析の目的でイベント現場にも導入が進んでおり、我が国では2020年の東京五輪開催に向けて更なる普及が予想されている。監視カメラの高画質化、映像処理技術の進展によっ

て、カメラ映像の解析技術の実用化が進んでおり、混雑状態解析に適用する方式も報告されている⁽¹⁾。

従来の混雑状態の映像解析では、個々のカメラ映像から混雑状況を検出する解析精度向上を主たる目的に研究がなされている。しかし、雑踏警備では、個別のカメラ映像の精度よりも、監視範囲全体の人の流れ(人流)とその変化の把握が重要である。さらに、精度向上を目指す方式では、映像中の人物認識に基づく方法など、一般に演算量が大きく高性能サーバでの処理が必要になる。解析をサーバで行う場合、多数のカメラからのリアルタイム映像伝送を保証する広帯域通信路、つまり有線通信が必要となる。このような設備をイベントごとに期間中のみ設置することは、コストがかかり、特に有線通信は設置条件からも現実的ではない。

そこで、映像解析を活用する警備支援システムとして、次を目標として開発している。

(1) 解析手法の目標

- 個別のカメラ映像範囲の人数把握ではなく、経路上での人流量を検出できること
- 人流量が増加・減少したのか、増加によって移動が困難で雑踏事故リスクが高い滞留が生じているのかを検知できること
- これらの検知が、カメラ設置条件などによらずロバストに行えること

(2) システム構築上の目標

- 映像解析は、カメラ内、又はカメラ側に併設される機器上で実現可能な処理量であること
- 解析結果は十分に少ないデータ量であり、警備本部で目視する場合に必要な一部のカメラからのリアルタイム映像伝送と併せて、無線通信によってシステムが構築できること
- イベント規模に応じた柔軟な構成がとれること

(3) 情報提供手法の目標

- 人流、滞留情報の位置、時間変化などを、警備員にとって容易に判断・予測可能な可視化情報として提供できること(図1)

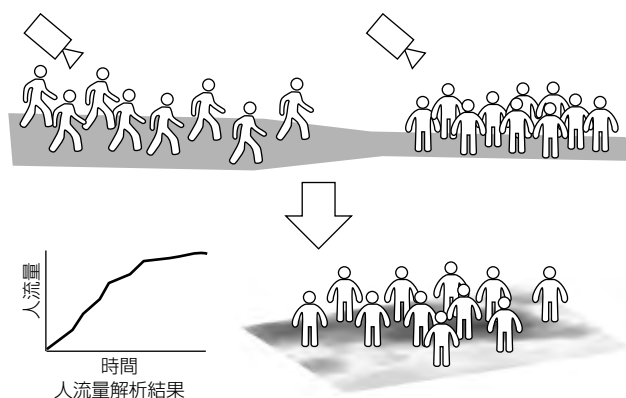


図1. 混雑状況の可視化

これらを満足する映像解析技術として、動き情報に基づく人流量解析方式と、滞留検知方式を提案する。動き情報は映像の連続するフレーム間での物体の動きを大きさと方向で表現したものである。動き情報としては、映像の圧縮符号化の過程で抽出される符号化情報としての動きベクトルと、画素ベースで動きを抽出するオプティカルフローがある。動き情報を用いて映像の特定の位置を通過する映像特徴量の評価によって人流量推定を、時間的な特性の変化から、滞留を検知する。

これらの方式では、映像の大局的特徴からの推定であり、個々のフレーム内の人物認識によって人流量や滞留を解析する方法に比べ、精度向上は困難であるものの、安価なプロセッサを追加することでカメラ内、又はカメラ側の機器実装が可能である。さらに、映像のフレーム間の変化に着目した方式であるため、カメラの設置位置や方向、背景画面、天候などの影響を受けにくく、人が前景として撮影されているかぎり、環境に対して頑健な検出が可能であると考えられる。

さらに、人流量、滞留判定結果という映像データに比較して極めて少量の解析データのみを警備本部側システムに伝送すればよく、その解析データ量は時間的な変動が小さいことから、無線伝送の品質上多少のパケットロスがあっても、警備本部の状況把握に影響が出ることはない。

3. 混雑状態解析技術

この章では、イベント警備支援を目的とした混雑状態解析技術について述べる。解析対象とする混雑状態を示すパラメータは人流量、滞留状態の2種類である。

3.1 人流量解析方式

映像のフレーム間の変化量であるオプティカルフローを利用して経路上の人流量を推定する。基本的な考え方は、映像内で人が歩行していれば、歩行方向に人の面積に対応する前景の動きがオプティカルフローとして観測されるというものである⁽²⁾。

しかし、この手法が対象とする雑踏警備のための監視カメラ映像では、前景面積と人流量は比例しない。監視カメラは多くの場合、群集を斜め上方から撮影する。この撮影条件では、群集の密度が低い場合には、個々の歩行者が個別に観測されるが、高密度群集では、歩行者同士の重なりあい、すなわちオクルージョンが高い頻度で発生することが予想されるため、前景面積と人流量は比例しなくなる。そこで、前景面積と群集密度の関係の分析に基づき、人流量を推定することで、オクルージョンの影響を除外する。

前景抽出処理では、次の歩行者の振る舞いの性質に注目することで処理負荷低減と精度向上を果たしている。

- (1) 移動方向は経路に沿った一方向又は二方向である。
- (2) 混雑に伴い(群集密度1.5人/m²超)、歩行者同士の追

い抜きが困難になるため⁽³⁾、群集密度及び移動速度が一樣となり、時間経過に伴う群集内の歩行者の位置関係の変化が小さくなる。

(1)の性質によって、経路と交差する部分領域のみを処理対象としても、経路を通過する群集を漏れなく解析できる。また(2)の性質によって、部分領域で取得した群集特徴量の時系列データは、部分領域を通過した群集を映像全体を空間的に捉えた特徴量とみなすことが可能になる。例えば1 m/sで移動する群集の前景面積を前記部分領域で10秒間観測した場合、移動方向に10m分の群集の前景面積を取得したものとみなせる。フレームごとの画像処理対象範囲を狭い画像領域に限定できるため、処理量を大きく低減することができる。また狭い画像領域内では群集の撮影角度やスケールの変動が少ないため、歩行者一人に対応する前景面積が安定し、人流量解析の精度向上が期待できる。

前景面積と群集密度の関係は、歩行者同士のオクルージョンの割合を群集密度ごとに求めることで導出した。オクルージョンの割合は、群集密度に対して定まる歩行者間の距離、歩行者の平均寸法及び監視カメラの俯角(ふかく)から導出した。

この考え方に基づき、次に示す4つのステップで人流量を解析する(図2)。

- ステップ1：経路と交差するラインをあらかじめ設定する。
- ステップ2：その周辺の部分領域のオプティカルフローを各フレームに対して算出する。
- ステップ3：ラインをまたぐオプティカルフローを持つ画素集合を、オプティカルフローの方向別に前景として各フレームで抽出する。
- ステップ4：抽出した前景の面積をフレーム分累計し、前景面積と群集密度の関係から、前景面積よりフレームにラインを通過した歩行者数を方向別に推定する。

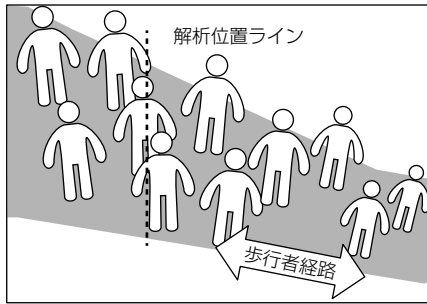
歩行者経路を移動する群集を100分間撮影した映像を用いて提案方式の性能評価を行った。評価映像は10fps、400×250ピクセルの動画像である。撮影時の監視カメラ俯角は60°、また最も人流量の大きい時間帯で、目視で確認した群集密度は2人/m²であった。

各時刻における人流量を往路方向と復路方向別に解析した結果を図3に示す。どちらの時刻でも、目視で取得した真値に近い人流量が得られた。また人流量の累計の真値からの誤差は9%であった。

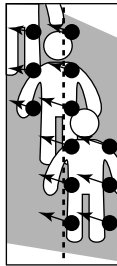
評価映像はほぼ全ての時間帯でオクルージョンが発生しており、また流量の増加に応じてオクルージョンの割合も高くなる状態であったものの、解析結果と真値がどちらの時刻でも一定の誤差範囲内で収まっており、オクルージョンの影響を除外して人流量が推定できていることを確認した。

これによって、歩行者同士のオクルージョンが発生する

ステップ1：あらかじめ歩行者経路と交差するラインで解析位置を設定



ステップ2：
オプティカルフロー算出



ステップ3：
ラインをまたぐ前景を抽出



ステップ4：Nフレーム分の前景面積から群集密度推定に基づき歩行者数を推定

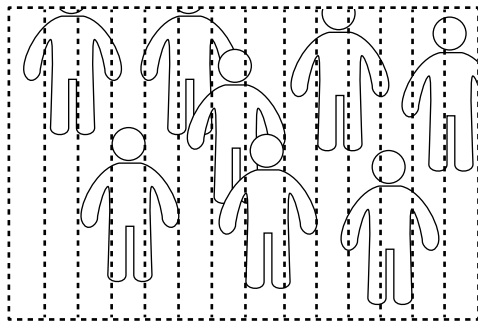


図2. 人流量解析手法

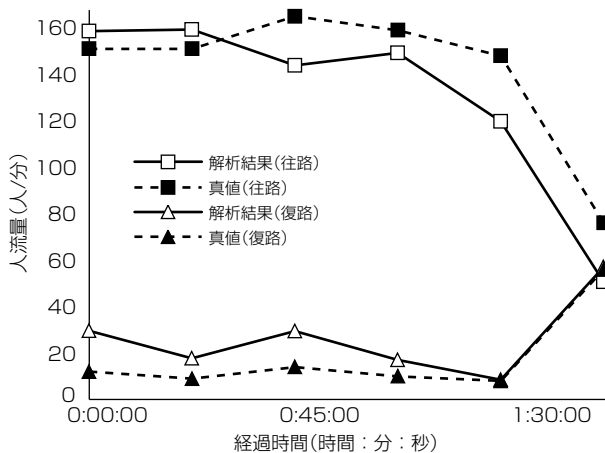


図3. 人流量解析結果

高密度群集に対して、誤差9%の人流量解析を実現した。今後は様々な撮影条件で提案手法の評価を行い、課題抽出と性能改善を実施していく。

3.2 滞留検知方式

群集が移動している場合には、映像からは映像の各領域

で一定方向の動き情報が検出される。一方、滞留が生じると、移動量は小さくなり、移動以外の人の動きによる局所的で方向が一定しない動き情報が観測される。そこで、群集映像から抽出した動き情報の時間的なバラつきを乱雑度と定義し、その度合いから滞留を検知する方式を開発した⁽⁴⁾。また、この方式では圧縮符号化時の動きベクトルを映像の動き情報として用いることで処理負荷の軽減を図った。

乱雑度 ε を式(1)のように定義する。

$$\varepsilon(x, y, T) = \left(\left| \sum_{t=NT}^{N(T+1)-1} \frac{\bar{v}_t(x, y)}{|\bar{v}_t(x, y)|} \right| \right)^{-1} \dots\dots\dots (1)$$

ここで、 (x, y) は乱雑度を計算する画素ブロックの位置座標であり、 $\varepsilon(x, y, T)$ は画素ブロック単位で求められる。これは、符号化時に得られる動きベクトルが画素ブロック単位で算出されることに由来し、現在の監視カメラに広く用いられているH.264符号化方式の場合、画素ブロックの最小単位は 4×4 ピクセルである。 N は乱雑度を計算するフレーム数、 T は映像を N フレーム単位で区切ったときのインデックス番号、 $\bar{v}_t(x, y)$ は画素ブロックにおける t フレーム目の動きベクトルである。

この方式では、動きベクトル $\bar{v}_t(x, y)$ を連続する N フレームにわたって合成し、合成ベクトルノルムの逆数を乱雑度 $\varepsilon(x, y, T)$ として定義する。このとき、動きベクトル $\bar{v}_t(x, y)$ を単位ベクトル化して合成することで、映像の奥行きによって生じる動きベクトルのスケール差や、突発的に発生するノイズの影響を軽減する。 $\bar{v}_t(x, y)$ の偏角が時間的にバラついている場合、すなわち映像中の群集が滞留状態にある場合、合成後のベクトルノルムは小さくなるため、 $\varepsilon(x, y, T)$ は大きくなる。一方、 $\bar{v}_t(x, y)$ の偏角が一定方向に偏っている場合、すなわち映像中の群集がスムーズに流れている場合、合成後のベクトルノルムは大きくなり、 $\varepsilon(x, y, T)$ は小さくなる。

この方式では、次に示す3つのステップで滞留を検知する(図4)。

ステップ1：監視カメラ映像の符号化情報から動きベクトルフレーム分を抽出する。

ステップ2：抽出した動きベクトルのうち、同一箇所にある動きベクトルから、乱雑度 $\varepsilon(x, y, T)$ を計算する。

ステップ3： $\varepsilon(x, y, T)$ から画素ブロックごとの滞留有無を判定し、滞留ありと判定された画素ブロックの個数、位置関係、及び時間的な連続性を総合的に判定し、最終的な滞留有無を検知する。

この手法の有効性検証のため、滞留と解消を断続的に繰り返す群集映像を用い、滞留検知実験を行った。使用した映像の諸元を表1に示す。ここで滞留状態を、映像から切り出した 225×225 ピクセルの領域で、連続するフレーム中で領域外への人の移動がない状態と定義する。今回は3秒

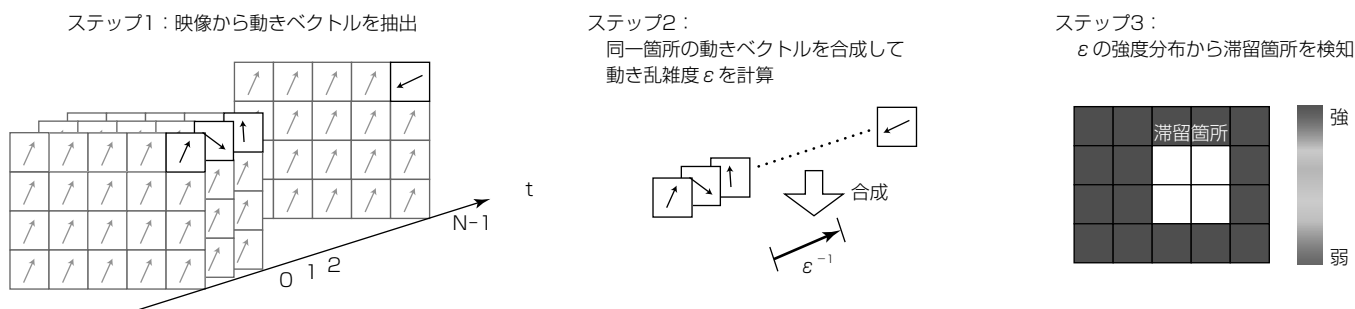


図4. 滞留検知手法

表1. 評価映像の諸元

項目	値
解像度(ピクセル)	1920×1080
長さ(min)	10
フレームレート(fps)	10

表2. 評価結果

評価総数784		目視で得られた滞留状態	
		滞留あり	滞留なし
検知結果	滞留あり	371	16
	滞留なし	35	362

単位で滞留を判定、すなわち $N=30$ とし、映像中から切り出した4つの領域で、目視で得られた滞留有無を真値として、この手法による検知結果の正解率を測った。評価結果を表2に示す。全検知結果784件に対する検知正解数は733件であり、検知精度は93%であった。

誤報及び失報原因を分析したところ、大半は滞留と解消の過渡段階でのエラーであり、その前後では正確に検知できていることから、時間的に連続する滞留状態を検知するという視点からは問題とはならないと考える。一方、システムの目的から、最も避けるべきエラーである滞留状態を検知できない失報35件について詳細分析した結果、7件のエラーは被写体の動きが小さい、又は輝度差が小さいなどの要因で、動きベクトルが検知されず、人がいない状態と同等と判断されたためのエラーであった。

これらの結果から、時間方向の処理などによる改善を行えば、十分に高い精度で滞留状態の検知が可能であると考ええる。今後はさらにカメラ設置位置、夜間、雨天、背景の状況などの種々の環境での性能検証と改良を行う。

4. む す び

従来の雑踏警備では現場の警備員からの主観的・定性的な情報を収集し判断するが、イベントの大規模化に伴い従

来手法での現場状況判断はますます困難になっている。この問題に対して、我々は、監視カメラ映像の解析結果に基づき、より適切な警備を可能にする警備支援システムに適用可能な映像解析技術を開発した。

開発技術によって、カメラ内での映像解析による混雑状態解析が可能になり、解析結果を地図上に多様な可視化を行うことで、混雑状況の把握ができる。また、解析結果のみを常時伝送することによって、イベント現場で構築可能な狭帯域なネットワーク環境下でも運用が可能となった。

今後は、映像解析方式の評価改良を行い、広域無線ネットワークの構築を可能にするマルチホップ無線技術⁽⁵⁾、複数のカメラ映像をシームレスに合成し監視者の見やすい視点からの映像の提供を可能にする俯瞰映像合成技術を適用してイベント警備支援システム開発を進めるとともに、雑踏の予測や人工知能技術を用いる誘導支援の開発も行い、雑踏警備のIT技術による質の向上と効率化を進めていく。

参 考 文 献

- (1) 上田昌治, ほか: 防災・広域監視, 映像情報メディア学会誌, **70**, No.1, 70~74 (2016)
- (2) 服部亮史, ほか: 混雑状態解析・可視化に基づくイベントセキュリティシステムの提案, 電子情報通信学会総合大会, D-12-41 (2016)
- (3) 貝辻正利: イベントを安心して楽しんでもらうために, 講談社エディトリアル (2014)
- (4) 西辻 崇, ほか: 動画像動きベクトルを用いた群衆の滞留検知, 電子情報通信学会総合大会, D-12-42 (2016)
- (5) 三菱電機ニュースリリース 2015年1月28日: 仮設用途対応監視カメラ向け無線ネットワークを開発
http://www.mitsubishielectric.co.jp/news/2015/0128-a_zoom_02.html

ホームネットワークの進化とIoT

三木智子*

Evolution of Home Network and IoT

Satoko Miki

要 旨

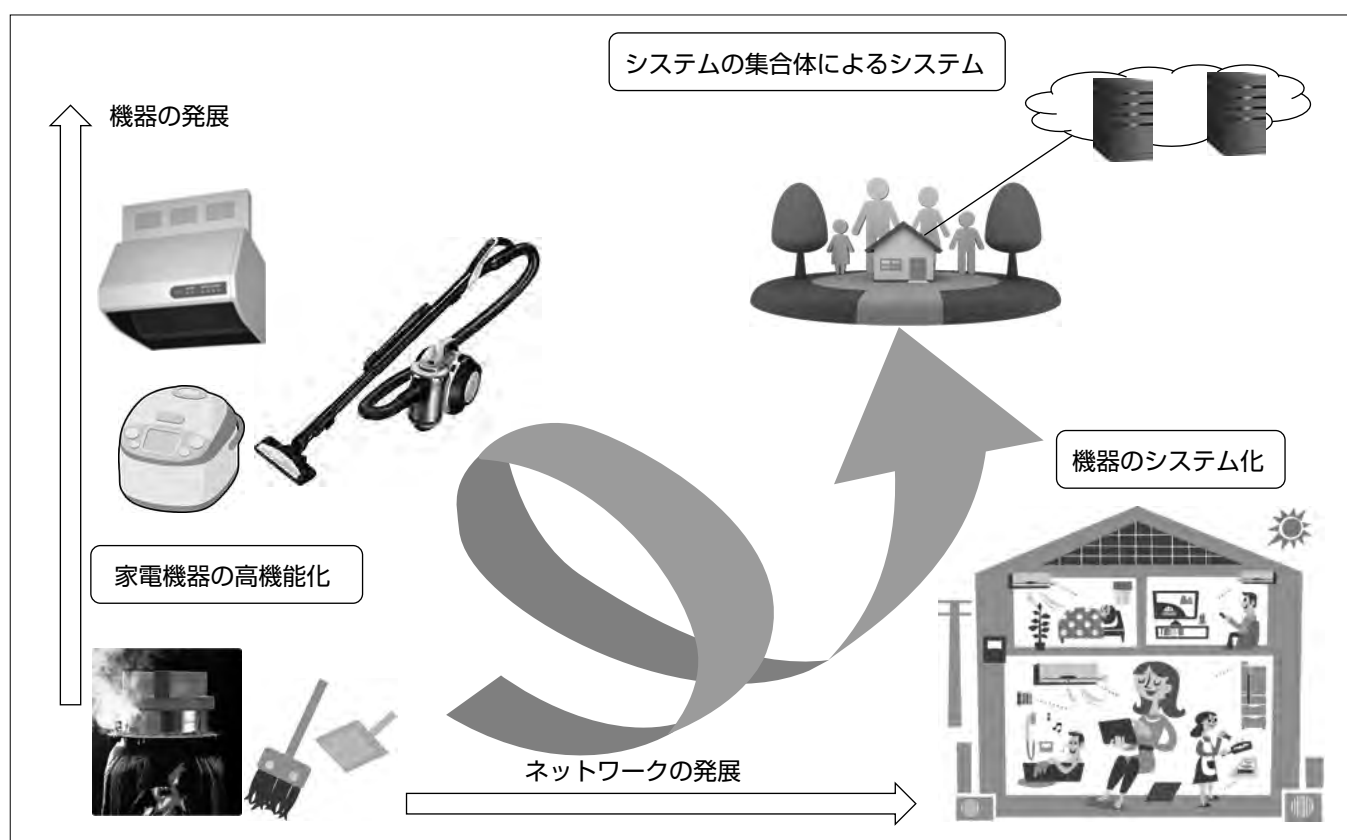
機器がネットワークにつながるIoT(Internet of Things)でこれまでのホームネットワークが新たな立ち上がりを見せている。ホームネットワークは、2010年頃から家庭内の映像機器を中心に動画や写真を共有するシステムとして始まり、その後、家電機器の電力消費量表示や外出先から自宅の家電機器制御でエネルギーを管理するHEMS(Home Energy Management System)へと拡大し、さらに、家のあらゆるモノがネットワークにつながる家のIoTへと進化している。

家での暮らしは、炊事、洗濯、掃除に始まり、電気・ガスなどのエネルギー消費や健康管理、子育て・教育、介護、娯楽、家族や地域とのコミュニケーションまで多くを含ん

だコト(真価)であり、生きることそのものである。

この家での暮らしの質を上げるために、それらをサポートする家事支援を価値と位置付け、三菱電機では、この価値を実現するための家電機器とネットワークの進化に向けて、家電機器の高機能化、機器のシステム化による快適性と省エネルギーの実現、システムの集合体による家とクラウドの全体のシステム化による家事支援のための技術開発に取り組んでいる。

今後、家電機器群のシステムオブシステムズに向かって、らせん状に進化していくホームネットワークを、IoTを活用した技術開発を行い、家事支援という価値を追求していく。



ホームネットワークの進化

ホームネットワークは、機器の発展とネットワークの発展によって、家電機器の高機能化、機器のシステム化、システムの集合体によるシステムとらせん状に進化していく。

1. ま え が き

ホームネットワークがIoTの社会実装形態の1つとして何度目かの注目を浴びている。IoTとは、様々なモノがインターネットにつながることであり、モノのデータが社会へ流通することである。IoTで収集されるデータを処理・解析することによって付加価値が生み出され、この価値が実世界に変化を与え、その変化が更に情報として収集される。この現象を家を中心に切り取ると、家電機器を含めた様々なモノのデータから価値を生み出し、その価値が社会を変化させると再定義される。

本稿では、家とそこに住む人の価値について述べ、人とモノの進化を支援する当社の取組みと今後の研究についてネットワークの進化との関連を示しながら述べる。

2. 家と家事とIoT

ホームネットワークの“ホーム”は、“家”であるが建造物だけではなくそこに住む人とその営み全般としての“暮らし”を意味している。例えば、人の暮らしは、朝、ご飯の炊けるにおいで目覚め、職場や出張先で仕事をし、家に帰って、お風呂でくつろぐ。ショッピングやジムでのスポーツなども暮らしの一部である。すなわち、暮らしとは、炊事、洗濯、掃除に始まり、電気・ガスなどのエネルギー消費や健康管理、子育て・教育、介護、娯楽、さらに家族や地域とのコミュニケーションまで含む人の生きる意味をなすことの多くを含んでおり、その主体は人である。であれば、家事とは暮らしをなすこれらの様々なものを含んだコト(真価)であり、生きることそのものでもある。それがゆえに多くの時間と作業を強いられることでもある。

先進国では、これまでにないスピードで少子高齢化が進展しており、これに伴う生産年齢人口の減少と人手不足の増大が課題となっている。特に日本では、2013年10月1日時点で65歳以上の高齢者人口は過去最高の3,190万人を超え、総人口に占める割合(高齢化率)も25.1%と過去最高を記録した。生産年齢人口も減少を続けており、8,000万人を割り込み7,901万人となっている。

こうした課題に向け、技術で家事支援を行うことが解決のアプローチの1つになり得る。過去を振り返ると、洗濯という家事を手助けする洗濯機は、手で回転させる攪拌(かくはん)式洗濯機から始まり、1908年にアメリカで電気式洗濯機が発明され、全自動、ドラム式と進化を遂げているが、これは、洗濯という重労働を科学技術で代替するモノである。すなわち、家電機器は“人の行っている家事をエンジニアリングシステムで代替するモノ”と捉えることができる。これが、これまでの家庭にある電気機器の価値である。

今世紀に入って家電機器はネットワークにつながってき

ている。

家電機器を含めて様々なモノがインターネットにつながることがIoTである。センサ等によって現実社会がデジタルデータ化され、そのデータがネットワークに流通する。IoTは、実世界のあらゆるモノに関するデータがデジタル化されることを意味しており、さらに、これが収集・蓄積され、データが処理・解析されて新たな価値が生み出される。この価値が再度実世界に変化を与え、この変化もまたデータとして収集される仕組みを実現する要素となる。こうした中、人の暮らしに労働を強いてきた家事のうち義務感や重圧を感じている作業をエンジニアリング、特にIoTの技術を用いて軽減していくことで、生産人口の労働時間や労働への活力となる余暇時間を生むことが可能になると考える。

当社では、家事支援を実現するための技術的解決方法としてIoTを駆使した機器やシステムの検討を行っている。本稿では、ホームネットワークの進化をIoT、ネットワーク化の仕組みの中で考え、まず、①家電機器の高機能化としての家電機器のネットワーク、次に、②機器のシステム化としての進化した家電機器群のホームネットワーク、さらに、③システムの集合体による家全体のシステムとしての家電機器群のホームネットワークについて述べる。特に③では、ホームネットワークのシステム・オブ・システムズがどのように家事支援を行っていくかについて述べる。

3. 家事支援のためのIoT

3.1 家電機器の高機能化

2章で述べたように家電機器は、“人の行っている家事をエンジニアリングシステムで代替するモノ”である。すなわち、機器を利用してユーザーが目的機能値を設定、操作し、機器が自ら環境や状況を理解して機能する。詳細には、環境情報の取得とそれに応じた機器状況の理解、機器状況に応じた適切な操作の決定と操作スケジューリング、さらにはその操作スケジューリングに基づく機器機能と分解される。

この定義と解釈では、機器と機能にネットワークの概念はない。ネットワークは“目的機能値の設定”“環境状況理解”“操作の決定と計画”“機器機能”での命令やデータ伝達のために使われ、機能が物理的に離れているときにそれらの間をつなぐ仕組みである。

ここでは、家電機器を機能と概念から述べたが、具体的な例として電気炊飯器を取り上げる。電気炊飯器は、薪(まき)拾いから薪割り、火起こしから始まる作業を電気によって支援する家事支援エンジニアリングシステムの雄である。炊飯は、おいしいご飯を食べるという価値を人に提供する。この電気炊飯器の進化を当社炊飯器を例にして述べる。電気炊飯器は、釜の素材にこだわるとと

もに、加熱にIH(Induction Heating)の技術を用いて、電気や磁力を利用して加熱する。また、デンプンが大きく変化するポイントである本炊き時に滞留を止めずに連続沸騰させることで、炊きあがりのおいしさを引き出すことができる。そこで、炊飯釜内部の沸騰を検知し、炊飯釜自体の温度が内容物の沸騰を検知したときの温度より高温になるようにして沸騰を維持させる沸騰維持制御を行っている⁽¹⁾(図1)。この炊飯器の例は、炊飯器という家電機器の進化であり、さらに、ネットワーク機能も持つようになってきている。炊飯器本体に近距離無線通信機能(Near Field radio Communication : NFC)を備え、スマートフォンなどのスマート端末のタッチ操作によって、炊飯器に目的機能の設定を行うものが存在する。ユーザーはスマート端末に炊き分けの条件を入力し、この情報を炊飯器本体に送信、設定して炊飯する。また、炊飯器本体から炊飯の状況データを取得してスマート端末に出力する。この例では、目的機能の設定と炊飯機能が物理的に離れて存在し、それをネットワークでつないでいる。これによって、ユーザーは新たに簡単な操作で炊飯器の機能を引き出して、よりおいしくお米を炊くという価値を得る。

3.2 機器のシステム化

この節では、進化した家電機器をネットワーク化して相互に家電機器群として快適でかつ効率よく機能させるための家電制御について述べる。

家の様々な家電機器をネットワークで接続し、エネルギーの“見える化”や状況に応じて機器を制御することによって快適で省エネルギーな暮らしを実現するシステムは、HEMSとして知られるところである。HEMSは、創エネルギー・蓄エネルギー・省エネルギーを、かしこく制御するシステムである。特に、当社では新たな試みとしてHEMSを使って空調や給湯に、換気システムを連動させる機能を開発している。例えば、冬期にエコキュートでお風呂の湯はりを開始すると、HEMSが浴室換気を抑えるように自動的に制御し、湯はり時に暖められた浴室の温度を有効に活用することで、入浴時にひやっとした感じのな

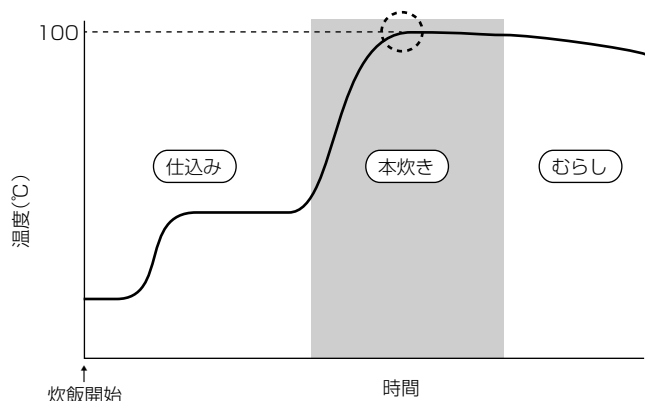


図1. 炊飯中の温度変化

い快適な浴室を実現する(図2)。また、レンジフードファンの運転と連動して換気風量を自動的に制御することで、必要以上に換気量が多くなってしまいう“過換気”の状態を解消することで、冬は不快な冷風感をなくすとともに、廃熱による暖房のムダを抑える効果がある。このように、家電機器を機器群として制御するホームネットワークが、単体の家電機器では成し得なかった新しい快適性やムダを抑える価値を提供する。

3.3 システムの集合体によるシステム

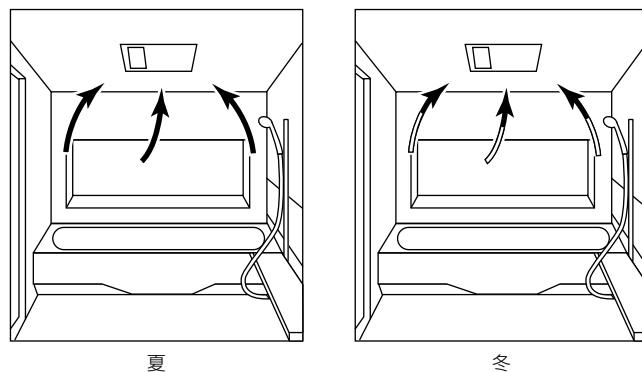
最後に、進化した家電機器群とシステムのネットワーク化によるホームシステムの将来について考察する。未来の家のありようとして、ホームシステムが家を越えてネットワークにつながり、1つのシステムを構成すると考えている。

この未来を実現するためには、広範な技術の連携・統合が必要になる。そこで、技術の連携・統合たるシステムがどのように構成され、どのように進化していくのかについて検討し、向かうべき未来に寄与する技術について研究を進めている。

3.2節で、機器群がネットワークで接続されることで新たな価値が生み出される例について述べた。ネットワークにつながるシステムでは、1つのノードから出ているリンクの数を横軸に、その数を持つノードの数を縦軸にプロットすると、両対数グラフで傾きが負の直線となる。す



(a) 換気連動設定



(b) 換気風量で温度低下を抑制

図2. 湯はりと換気の連携

なわち，“リンクの数が2倍になるごとに，その数のリンクを持つノード数はほぼ1/5に減少する”というべき乗則が現れる⁽²⁾。また，インターネットは，同一対象について時間や空間的に異なるスケール(分解能)で計測された統計が同じ分布族に従い，分布やモーメント等の統計的性質が計測スケールに関して相似であるという統計的に自己相似となっていることが報告されている⁽³⁾⁽⁴⁾。べき乗則が成り立ち，また，自己相似であることは，フラクタルの定義に合致し，ネットワークシステムは，全体から一部を切り取ってもそれが全体と似ている成り立ちをしていることが分かる。

次に，ネットワークでつないで行う処理について考えてみる。1970～1980年代には，処理はメインフレームと呼ばれるコンピュータがホストとなり，それにダム端末を用いて文字情報を入出力していた。ダム端末の処理能力が上がるにつれMS-DOS^(注1)やCP/M^(注2)などのOSが動く端末にホストのアプリケーションの一部機能が移されてきた。これが1990年代のクライアント／サーバ型の処理につながり，機器のオープン化，ダウンサイジング化を呼び起こした。さらに，現在，ネットワークの高速化とともにWebアプリケーションによるアプリケーション処理と出力処理の分離が起こり，クラウド化が進んでいる。これは，アプリケーションのオープン化であり，クラウドの処理比重が大きい。このように，処理能力とネットワークの進化でコンピューターシステムは，機器さらにはアプリケーションがオープン化しながら処理の比重が上位(クラウド)と下位(端末)とを行ったり来たりし，らせん状に発展してきている。

したがって，ネットワークでつながる処理システムは，ある時刻にそれぞれフラクタルな構成で散りばめられている処理が時間的には上位と下位に比重を振れながら進化していると考えられる。そうであるとすれば，機器とクラウドの進化スピードのバランスから，この次の世代では，機器の側に比重を移し，より下位の近傍で比較的大量の処理

が行われるホームシステムが形成されていくであろう。そして，最終的には，完全にフラクタルで比重が偏らない自律分散協調モデルになっていくと考えられる。そこで，次の世代のホームシステムとして，家又は家の近傍で価値を生み出す処理をするためのエッジコンピューティングの活用について開発を進めている。

進化した家電機器群とシステムのネットワーク化によるホームシステムは，家電機器としてそれぞれ炊事や買物をサポートする価値を持ちながら，IHクッキングヒーターの使用と冷蔵庫の使用から食事の提案や健康サポートなど，暮らしそのものの質を向上させ，家事支援という価値を提供していくであろう。

(注1) MS-DOSは，Microsoft Corp. の登録商標である。

(注2) CP/Mは，(株)技術少年出版の登録商標である。

4. む す び

ホームネットワークは“IoTという手段を持って，人の行っている家事をエンジニアリングシステムで代替するコト”である。家事労働を軽減し，これまでにない，暮らしの提供を目指す家事支援という価値をIoTと情報・通信技術で解決していく。

参 考 文 献

- (1) 特許第4611415：加熱調理器 (2010)
- (2) マーク・ブキャナン：複雑な世界，単純な法則，草思社 (2005)
- (3) Leland, W.E., et al.: On the self-similar nature of Ethernet traffic, IEEE/ACM Transactions on Networking, **2**, No.1, 1～15 (1994)
- (4) Koucheryary, Y., et al.(Eds): Next generation teletraffic and wired/wireless advanced networking, Proc. of 6th International Conference NEW2AN 2006 (2006)

高信頼・低遅延な無線通信技術

青山哲也* 木下裕介*
鈴木和雅* 武 啓二郎**
梅田周作*

Reliable and Low-latency Technologies for Wireless Communication

Tetsuya Aoyama, Kazumasa Suzuki, Shusaku Umeda, Yusuke Kinoshita, Keiji Take

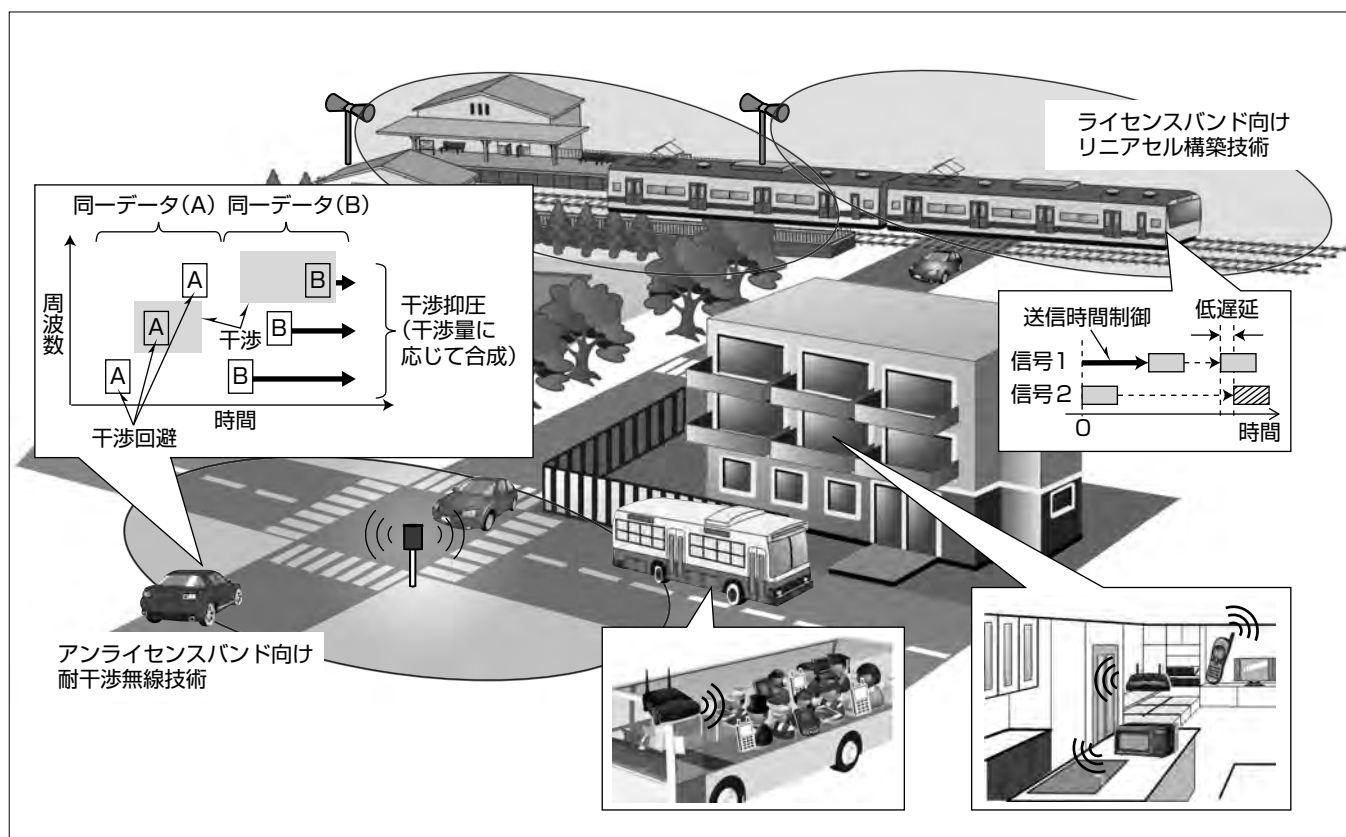
要 旨

様々なモノがセンサと無線通信を介してインターネットの一部を構成するIoT(Internet of Things)では、道路や鉄道、ビルや工場、橋などの社会インフラに設置された機器を、無線通信によって接続し、収集した様々なデータを分析することで、新たな価値を創出することが期待されている。設置利便性やリアルタイム性、信頼性が必要となる社会インフラ全体にIoT化を進めるには、高信頼・低遅延な無線通信技術が求められる。

無線通信は、無線局の免許が必要なライセンスバンドを用いるものと、一定の規格を満たすことで無線局の免許が不要なアンライセンスバンドを用いるものに分けられる。

社会インフラ全体にIoT化を進めるには、ライセンスバンドとアンライセンスバンドのそれぞれを用途によって使い分けるとともに、高信頼・低遅延化技術の適用が必要となる。

ライセンスバンド向けのリニアセル構築技術は、鉄道や高速道路等の高速移動体向けに、ミリ波帯の持つ直進性にセル内／セル間干渉対策を行うことで大容量、高信頼な無線通信を実現する。アンライセンスバンド向けの耐干渉無線技術は、干渉回避と干渉抑圧によって無線LAN(Local Area Network)等のアンライセンスバンドを用いる機器からの電波干渉に対する耐性を高めた高信頼無線通信を実現する。



社会全体のIoT化を支える高信頼・低遅延な無線通信

鉄道や高速道路等の高速移動体向けにミリ波を用いたライセンスバンド向けリニアセル構築技術と、干渉回避と干渉抑圧によって無線LAN等からの電波干渉に対する耐性を高めたアンライセンスバンド向け耐干渉無線技術によって、高信頼・低遅延な無線通信を実現する。

1. ま え が き

様々なモノがセンサと無線通信を介してインターネットの一部を構成するIoTでは、道路や鉄道、ビルや工場、橋などに設置された機器を、ネットワークを介して接続し、収集した様々なデータを分析することで、新たな価値を創出することが期待されている。社会インフラの基盤となる制御システムでは、リアルタイム性や信頼性が求められることから、従来は伝送路の外乱対策として有線によるネットワーク化が進められていた。今後は設置の利便性や、移動環境も含めた社会インフラ全体のネットワーク化の観点から無線化が進められ、これに伴い高信頼・低遅延な技術が求められる。

無線通信システムは、無線局の免許が必要なライセンスバンドを用いるものと、一定の規格を満たすことで無線局の免許が不要なアンライセンスバンドを用いるものに大きく分けられる。ライセンスバンドを用いるシステムとしては、携帯電話や列車無線等の移動体通信が知られている。アンライセンスバンドを用いるシステムとしては、無線LANやBluetooth^(注1)、ZigBee^(注2)、Wi-SUN^(注3) (Wireless Smart Utility Network)などが知られている。

IoT化を推進する上で、社会インフラ全体のネットワーク化を進めるためには、ライセンスバンドとアンライセンスバンドのそれぞれを用途によって使い分けるとともに、高信頼・低遅延化技術の適用が必要である。

本稿では、高信頼・低遅延な無線技術として、ライセンスバンド向けのリニアセル構築技術と、アンライセンスバンド向けの耐干渉無線技術について述べる。

(注1) Bluetoothは、Bluetooth SIG, Inc. の登録商標である。
 (注2) ZigBeeは、ZigBee Alliance, Inc. の登録商標である。
 (注3) Wi-SUNは、Wi-SUN Allianceの登録商標である。

2. ライセンスバンドにおける高信頼・低遅延化

2.1 ミリ波リニアセルコンセプト

ライセンスバンドを用いた専用無線通信システムの1つ

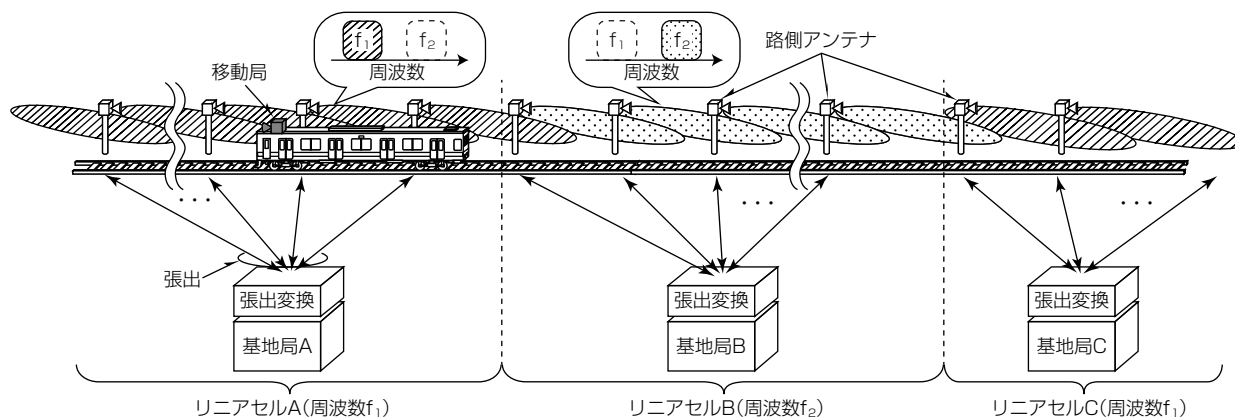


図1. ミリ波リニアセルコンセプト

である列車無線では、従来の音声通話サービスに加え、列車各部の機器状態のリアルタイムモニタリングやセキュリティを目的とした監視映像の伝送などの新たなアプリケーションも期待されており、列車無線システムの更なる大容量化、高信頼化への対応を進める必要がある。

大容量化に向けた三菱電機の一組みの一例であるミリ波リニアセルコンセプトを図1に示す⁽¹⁾。ミリ波帯はマイクロ波帯に比べて、①伝搬減衰が大きい、②直進性が高いという特徴があるが、伝搬減衰に対してはアンテナの指向性利得によって補填することが可能であるため、ミリ波が持つ直進性の高さを活用した、高速道路や鉄道等の高速移動体向けのミリ波通信システムを検討している。

アンテナごとに基地局を設置する従来のシステム構成では、干渉を避けるため短い距離で周波数の分割・切替えが必要であり、高速伝送が難しいという問題があった。また、基地局数が多くなることで、コストが増大するとともに、接続先の基地局を切り替えるハンドオーバーの回数が多くなる問題があった。これに対し、当社では多数の路側アンテナを1つの基地局に接続し、仮想的に大きなリニアセルを構成する。これによって、基地局間の距離が大きく取れるため、周波数の再利用が可能となり、2周波数繰り返して全線のサービスが実現できる。このため、基地局数の削減とともに、基地局当たりの周波数帯域幅を広くとることができ、高速伝送が可能となる。しかし、一方で、セル内及び近隣セル間における電波干渉問題への対策が必要である。次に、当社の対策技術を述べる⁽²⁾。

2.2 セル内干渉対策

セルサイズを大きくしたりリニアセルでは、同一セル内の路側アンテナから放射される信号に起因した長遅延波によってセル内干渉が発生する（図2の対策前）。このセル内干渉の影響をなくすために十分に長いガード区間を用意することも可能であるが、トレードオフとしてシステムスループットの低下を招くこととなる。

そこで、このセル内干渉対策として、各路側アンテナで敷設条件から決定される固定の送信遅延を与えることで、

移動局が信号を受信するタイミングを一定時間内に収める対策(図2の対策後)を検討している。これによって、符号間干渉用のガード区間を短縮することができる。

2.3 近隣セル間干渉対策

2周波繰返しでは、同一周波数を用いる近隣セル間でセル間干渉が生じる。これは、特に伝搬減衰の小さくなる晴天環境で顕著であり、セル端近傍のアンテナほどセル間干渉の影響は大きくなる。

この問題を解決するため、各路側アンテナにおける送信電力制御の適用を検討している。具体的には、路側アンテナが一方向に指向性を形成することを利用し、各アンテナの送信電力を傾斜配分する(図3)。

路側アンテナによって形成される受信電界は、自セルでは所望信号レベル、近傍セルでは干渉信号レベルとなる。受信点での信号品質を確保するため、①近傍セルからの被干渉が大きい地点におけるアンテナの送信電力を大きくし、②近傍セルへの与干渉が大きいアンテナの送信電力を小さくするように電力配分する。また、降雨環境で、雑音レベルを考慮したSINR(Signal-to-Interference-plus-Noise power Ratio)が要求レベルに満たない場合は、その分の送信電力も調整する。

2.4 セル内／セル間干渉軽減効果

セル内干渉対策と近隣セル間干渉対策の効果を、アンテナ設置間隔を1,000m、セルサイズを10,000m、アンテナ利得を32.3dBiとしたモデルによって計算機シミュレ

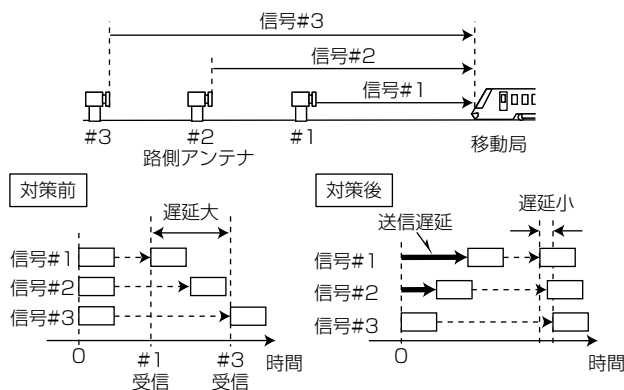


図2. セル内干渉対策

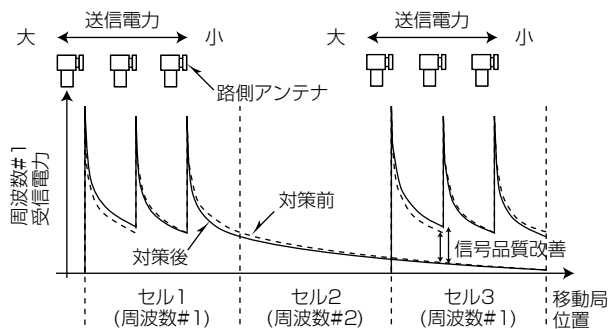


図3. セル間干渉対策

ションで評価した。

対策を行わない場合、セル内干渉対策のみ、セル内及びセル間干渉対策を適用した場合について、晴天環境における通信距離ごとの無線フレーム到達率特性を図4に示す。対策を行わない場合、通信距離が長くなるにつれて、符号間干渉が大きくなるため、無線フレーム到達率が低くなっているのが分かる。これに対し、セル内及びセル間干渉対策実施時は、全セル内で無線フレーム到達率ほぼ100%を達成できることが分かる。

3. アンライセンスバンドにおける高信頼・低遅延化

無線LANを始めとするアンライセンスバンドは、一定の基準を満たすことで自由に使うことができるため、無線機器が互いに電波干渉源となり、通信が途切れることが多かった。このため、リアルタイム性や信頼性が求められる産業機器の接続には無線LANを始めとする汎用的な無線通信は利用されることが少なかった。例えば、無線LANでは、自局がデータを送信する際に、周囲の電波環境を測定し、他局が通信を行っていないタイミングで送信するキャリアセンスと呼ばれる機能がある。狭い範囲で多くの無線LANを利用する場合、キャリアセンスによって大きな伝送遅延が発生してしまう。

この章では、アンライセンスバンドで高信頼・低遅延を実現するための耐干渉無線技術として、図5に示す周波数ホッピングによる衝突回避である干渉回避と干渉量に応じた合成である干渉抑圧について述べる。

3.1 周波数ホッピングによる衝突回避(干渉回避)

干渉回避は、使用する帯域(チャネル)を時間ごとに切り替え、単位時間当たりのスペクトルを拡散する手法で、同一周波数を利用し続ける方式と比べて雑音耐性を向上させることが可能である⁽³⁾。

一例として、帯域幅1MHz、1msのパケットを50msごとに周波数ホッピングを行う通信方式について検証し、実環境で取得したスペクトログラムと重ね合わせたものを

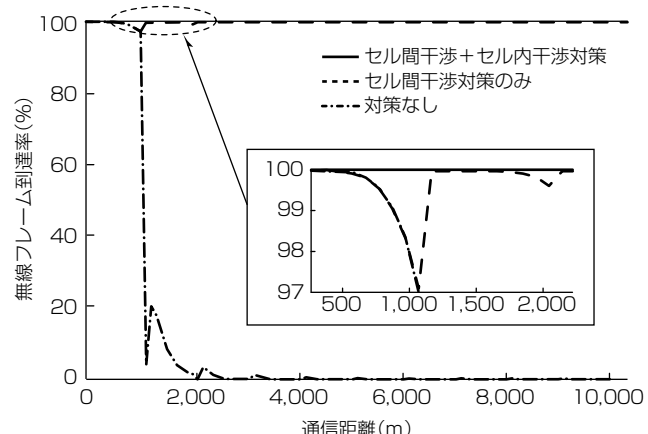


図4. 無線フレーム到達率特性

図6に示す。

周波数ホッピングを5回行い、5回とも-90dBm以上の干渉レベルを検知した場合を伝送不良と定義し、ホッピングを行わないシステムとパケット衝突確率解析によって比較した結果を表1に示す。

この結果から、干渉回避によって伝送成功確率が約82.3%向上し、干渉回避の有効性が確認できる。

3.2 干渉量に応じた合成(干渉抑圧)

干渉抑圧は、地上デジタル放送や無線LANなどで採用される変調方式であるOFDM(Orthogonal Frequency-Division Multiplexing)をベースとし、データを重畳しないヌルシンボルを時間-周波数に分散配置し、受信側でこのヌルシンボルによって干渉量を測定し、干渉量に応じ

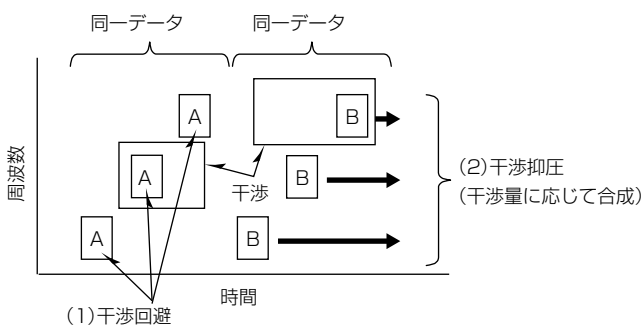


図5. アンライセンスバンド向け耐干渉無線技術

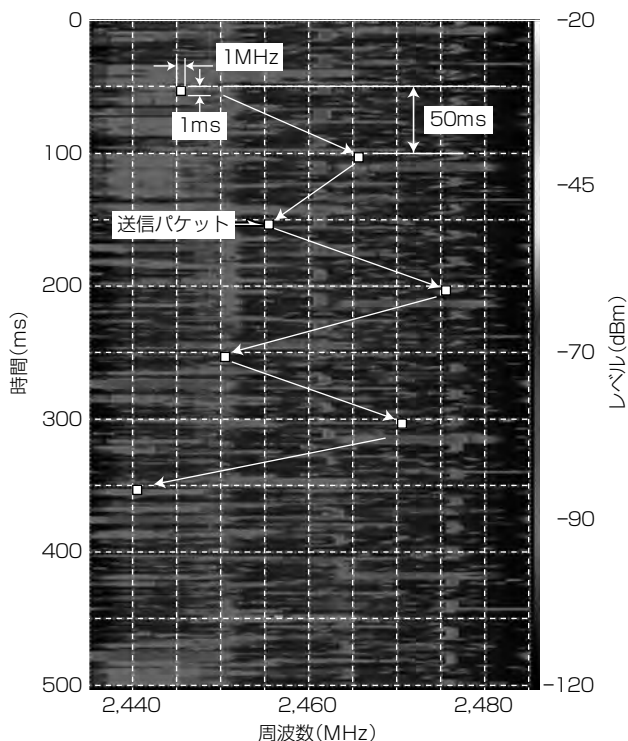


図6. 周波数ホッピングのシミュレーション例

表1. パケット衝突確率解析

通信方式	衝突確率(%)
常に同じ帯域を利用するシステム	0.130
干渉回避	0.023

てデータの重み付けを行うことによって干渉を抑圧する⁽⁴⁾。データを重畳しないヌルシンボルを配置することによって、自システムの信号と比較して高いレベルの干渉や、ダイナミックレンジの広い干渉に対して、精度の高い干渉量の測定が可能となる。また、ヌルシンボルを分散配置することによって、自システムの送信信号中のどこに衝突するか分からない短時間干渉や狭帯域干渉に対して、その存在を認識し、適切に対応することが可能になる。

3.2.1 ヌルシンボルの分散配置

一例として、4 OFDMシンボルに1つの割合で、データを重畳しないヌルシンボルを配置したイメージを図7に示す。ヌルシンボルの挿入量や挿入間隔は、自信号の帯域やシンボルレートと干渉の帯域や時間長との関係や、要求される伝送レートなどに応じて適切な値が決まる。ヌルシンボルの挿入位置は、受信側であらかじめ既知とする。サブキャリアへのデータのマッピング後、データ変調処理を行う。

3.2.2 干渉量の測定と重み付け

図8に干渉量の測定のイメージを示す。まず、着目しているデータシンボル(図8における黒塗りのシンボル)を含む4×4の領域内にある4つのヌルシンボルの平均電力を測定する。同様に、その周りの8つの4×4の領域のそれ

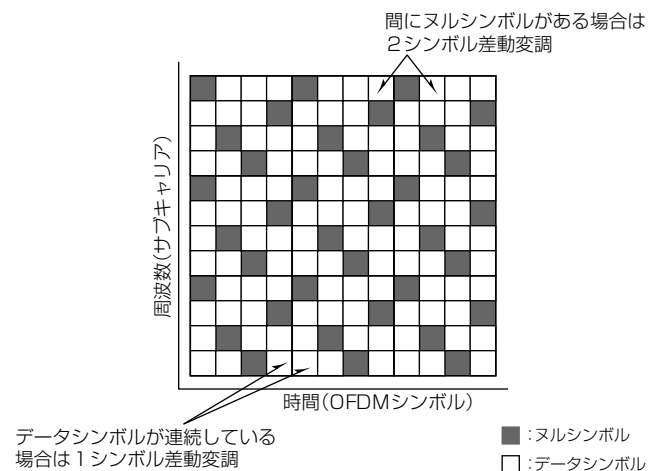


図7. ヌルシンボル配置のイメージ

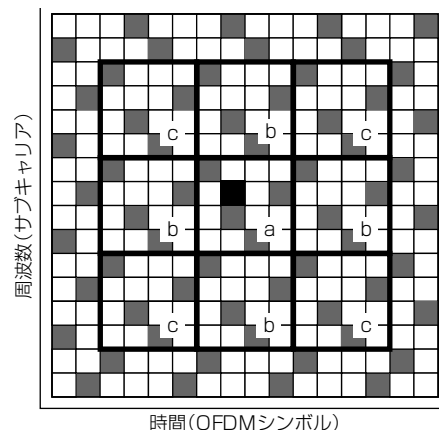


図8. 干渉量の測定

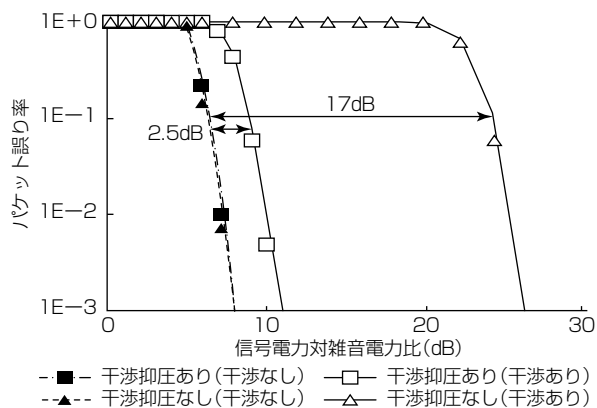


図9. パケット誤り率特性

表2. 干渉条件

項目	値
印加サブキャリア	1
干渉電力	雑音電力+28dB(干渉が衝突したサブキャリアでの電力)
印加時間	全OFDMシンボル

それぞれについて、ヌルシンボルの平均電力を測定する。そして、9つの4×4領域の干渉電力を図中のa, b, cの重み付けで加算することによって、時間-周波数の二次元フィルタを通した、このデータシンボルに対する干渉電力を算出する。

干渉量測定後、干渉量でデータシンボルの重み付けを行いながら、遅延検波を行う。干渉量による重み付けによって、例えば、大きな干渉が衝突したシンボルのデータは値が小さくなり、データの信頼度が低くなる。

3.2.3 干渉抑圧による効果

図9に、干渉量による重み付けを行う場合(干渉抑圧あり)と行わない場合(干渉抑圧なし)のそれぞれについて、表2の条件の干渉を加えた場合と加えない場合の1ビット当たりの信号電力対雑音電力比(E_b/N_0)に対するパケット誤り率(Packet Error Rate: PER)を示す。干渉抑圧なしの場合は、干渉を加えないときと比べ、干渉を加えたときは、PERが 10^{-1} を満たす E_b/N_0 で、特性が17dBと大きく劣化している。一方、干渉抑圧ありの場合は、干渉が多いデータシンボルの信頼度は低く、干渉が少ないデータシンボルの信頼度は高くなるようにデータシンボルの重み付けが行われるため、誤り訂正が効果的に働く。そのため、干渉を加えたときでも、加えないときと比べ、PERが 10^{-1} を満たす E_b/N_0 で、約2.5dBの特性の劣化に抑制できている。干渉抑圧なしの場合と比較すると14.5dBの差であり、この差は通信距離に換算すると、5倍以上の拡大に相当する。

4. 社会インフラ監視への適用

国内における道路・橋・トンネル・鉄道などの社会インフラは、高度経済成長期に集中して整備されたものが多く、近年、これらの老朽化が問題となっている。

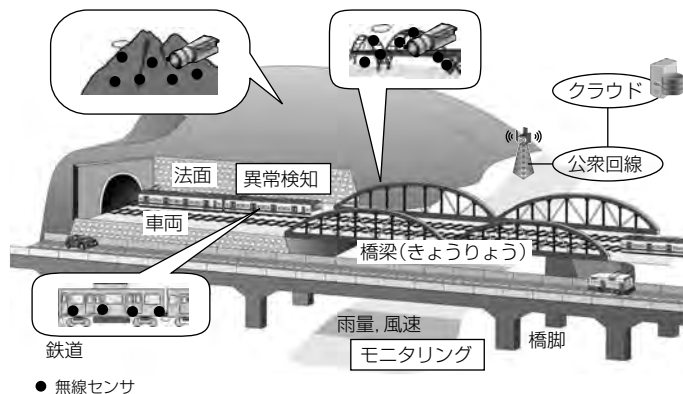


図10. 社会インフラ監視への適用

このため、これら社会インフラの点検・診断にセンサと無線通信を用いて予防保全や迅速な復旧活動を行う社会インフラ監視システムが期待されている(図10)。また、崖崩れや洪水などの自然災害はリアルタイムに検知する必要もある。例えば、多数の無線センサからデータサイズの小さな測定情報を収集する用途には、設置の自由度が高いアンライセンスバンドを活用し、一時収集拠点と監視拠点の間のような長距離伝送や高速移動環境、監視映像の伝送などの大容量通信の用途には、ミリ波のようなライセンスバンドを活用することが考えられる。ライセンスバンドとアンライセンスバンドを用途に応じて使い分け、それぞれに対して高信頼・低遅延な無線通信技術を適用した社会インフラ監視システムを構築することで、安心・安全な社会の実現に貢献していく。

5. む す び

IoT時代に向けて高信頼・低遅延を実現する無線通信技術について述べた。今後、これらの技術の移动通信環境への適用のほか、道路や鉄道、ビルや工場、橋などの社会インフラの監視への適用も視野に入れ、技術の展開を進めていく。

参 考 文 献

- (1) Nishimoto H., et al.: Millimeter-wave train radio communication system based on linear cell concept, Proc. of STECH2015, 1~12 (2015)
- (2) Umeda S., et al.: Cell structure for high-speed land-mobile communications, Proc. IEEE VTC2015-Fall, 1~5 (2015)
- (3) 小篠大輔, ほか: 電波環境測定データを用いたオフライン検証による高信頼無線方式の検討手法, 電子情報通信学会技術研究報告, DC2013-76 (2013)
- (4) 鈴木和雅, ほか: 耐干渉無線通信方式に関する検討, 電子情報通信学会技術研究報告, WBS2014-53 (2014)

IoTを支えるイーサネット規格 TSN技術

堀田善文* マンジン・クリストフ**
谷口幸子*
川手竜介*

Ethernet-based Time Sensitive Networking Technologies for IoT

Yoshifumi Hotta, Sachiko Taniguchi, Ryusuke Kawate, Christophe Mangin

要 旨

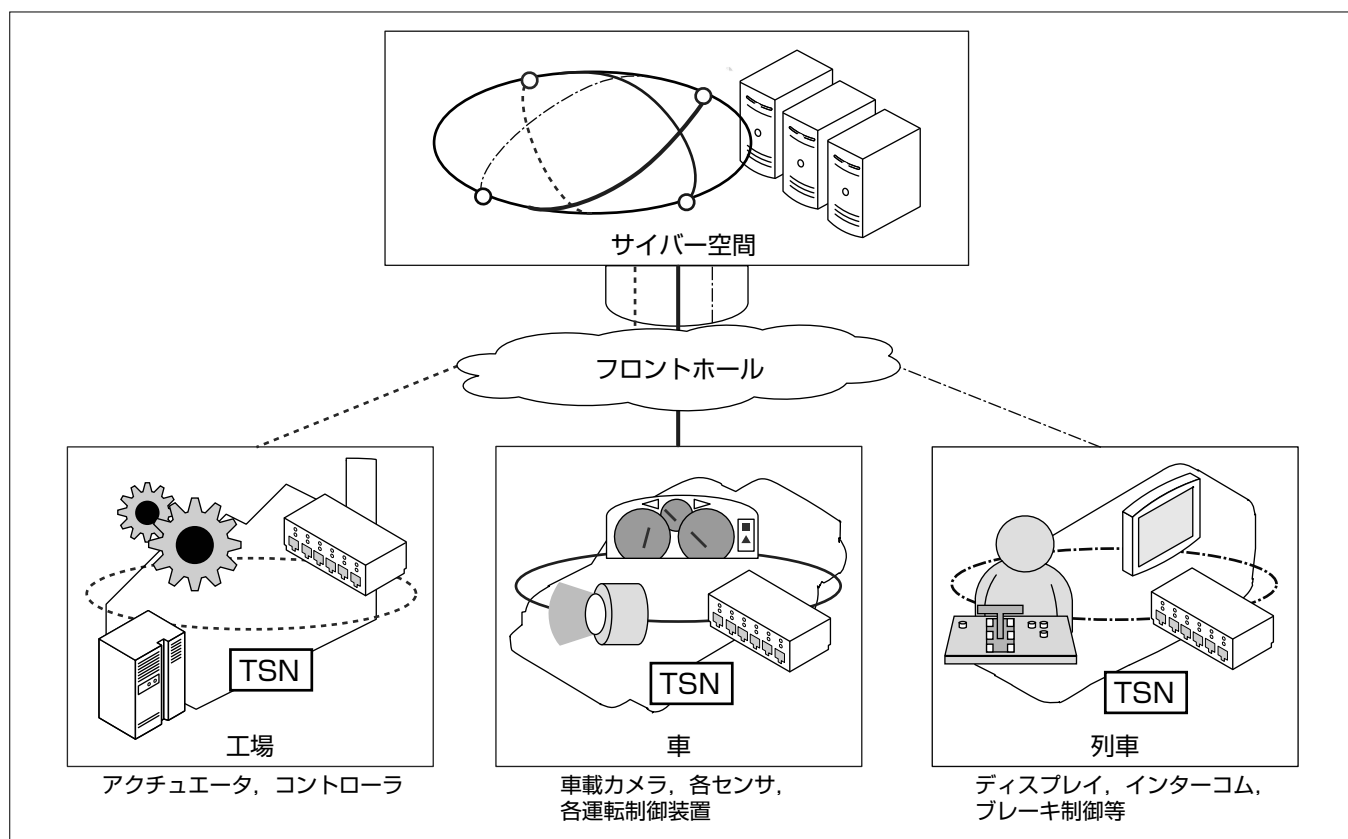
IoT(Internet of Things), M2M(Machine to Machine), CPS(Cyber Physical Systems)など、今までネットワーク化されてこなかったセンサ、アクチュエータ、コントローラがネットワーク化され、あらゆる情報をサイバー空間で収集・分析し、物理的な世界にフィードバックするための研究に世界中が取り組んでいる。これに伴い、従来それほど伝送遅延に配慮がいらないWeb, Eメール, 音声, 映像伝送のために使用されてきたイーサネット(注1)を始めとするネットワーク技術にも、アプリケーションによっては、伝送装置1台当たりの遅延が数 μ s以下という遅延制約が求められる時代が到来しつつある。

三菱電機では、低遅延アプリケーション向け通信規格で、IEEE 802.3及びIEEE 802.1ワーキンググループで標準

化されているTNS(Time Sensitive Networking)技術の1つでIEEE 802.3brに準拠したメディアアクセスコントロールを実装したイーサネット伝送装置の試作評価を行った。評価によって、多くの端末に使用され、イーサネット通信規格の中で最も汎用的な1 Gbpsの通信速度で、転送遅延を従来の22.90 μ sから3.52 μ sに抑えられることが分かった。

イーサネット規格TSN技術が世の中に普及することによって、従来技術では実現が難しかったIoT等を実現するための相互接続可能な汎用ネットワーク技術が確立され、2020年頃までに、産業機械、交通システム、自動車、通信インフラに普及していくものと考えられる。

(注1) イーサネットは、富士ゼロックス(株)の登録商標である。



多様なIoTサービスを集約する次世代ネットワーク

従来独自の低速なネットワークで接続されてきた工場内のデバイス、車載デバイス、列車内のコンポーネント類がインターネットにシームレスに接続されるようなネットワークが求められている。これらがネットワークに接続されることによって、多種多様なデータがサイバー空間に蓄積され、保守性や利便性、生産性向上に資する新たなサービスが生み出される。

1. ま え が き

工場・列車・自動車等の産業用ネットワークでは、これまで、接続される各機器の要求性能に応じた独自のネットワーク規格が混在している状況にあった⁽¹⁾。しかし近年、大容量化、経済化の観点から、産業用ネットワークのイーサネット化が進んでいる。

産業用ネットワークをイーサネット化すると、異なる遅延要求を持つ複数の機器やアプリケーションが同一ネットワーク内に収容され、低遅延転送が必要な制御系トラフィックと、比較的遅延を許容する情報系トラフィックが多重化される。しかし、イーサネットには産業用ネットワークで求められる低遅延性が不足しており、遅延要求の異なるデータを従来制御方式で多重化すると、制御系トラフィックの遅延時間が増大する場合があった。

本稿では、これらの課題を解決するために、近年検討が加速しているTSN技術の動向と試作評価の結果について述べる。

2. TSN技術の適用領域と課題

従来、イーサネットは大学や企業内の情報ネットワークに用いられており、工場・列車・自動車等の産業用ネットワークは、独自の閉鎖的なネットワークで単なる制御用途の機器のみを接続して運用されていた。近年これらのネットワークのイーサネット化が進んでいる。

例えば、工場の生産現場では、フィールドバス系の専用のネットワークに利用目的に合わせた独自のプロトコルを用いて制御するケースが多く、IEC61784やIEC61158などでCC-Link、PROFIBUS^(注2)、ControlNet^(注3)、INTERBUS^(注4)等、主に10Mbpsまでの多数のフィールドバス用オープン規格が存在していた。現在は、これらのフィールドバスがイーサネット化され、CC-Link IE、PROFINET^(注2)、EtherCAT^(注5)、EtherNet/IP^(注6)等、100M～1 Gbpsの多数の異なるフィールドネットワークの規格化が進んでいる。

また、列車の制御や情報伝送には、これまで多数の引通し線を並列に用いて機器を個別に制御していた。海外ではIEC61375 TCN(Train Control Network)のWTB(Wire Train Bus)やMVB(Multifunction Vehicle Bus)、国内では独自のトークンパッシング方式のバス等、主に10Mbps以下の専用バスが用いられてきた。2014年にIEC61375で100Mbpsのイーサネット規格であるETB(Ethernet Train Bus)やECN(Ethernet Consist Network)等の規格化が完了し、現在国内外で適用しようとする動きが加速しつつある。

車載ネットワークでは、LIN(Local Interconnect Network)やCAN(Controllor Area Network)、MOST(Media Oriented System Transport)等、20k～150Mbpsまでの

ネットワークが主流であり、近年インフォテイメント系で大容量の画像転送等に100M～1 Gbpsのイーサネットが使われ始めている。

先に述べたように様々な産業分野でイーサネット化が進んでいる理由は、IoTの時代に向けて、情報系から制御機器レベルまであらゆるものがつながり、シームレスなアクセスを可能にし、生産性・安全性・保守性・品質の向上や、省エネルギー化、低コスト化といったシステム全体の自動化及び最適化が期待されていることが挙げられる。したがって、画像や様々なセンサ情報等を大量に収集し、その情報を基に機器を分析・制御するためには、ネットワークを従来の10Mbps程度より大容量化することが求められる。イーサネットは既に10M～100Gbpsまでの規格化が完了し、400Gbpsが規格化中と、伝送速度のラインアップがそろっている。また、100Mbpsや1 Gbpsのイーサネットポートを持つ端末が増え、スイッチ等の通信機器の流量も多く、経済的であることもイーサネット化が進んでいる理由の1つであろう。

これらのイーサネット化が進み、制御系機器と情報系機器を1つのネットワークに収容することが可能になった場合、現場機器やセンサ、コントローラ等で扱われる遅延に厳しい制御系トラフィックと、WebアクセスやEメール等の比較的遅延を許容する情報系トラフィックが混在することになる。しかし、これらを従来のイーサネットスイッチで一般的なストア&フォワードで転送すると、同じ伝送路で転送が競合した場合、リアルタイム性が求められる制御系トラフィックの遅延が大きくなってしまう場合がある。例えば、一般的なイーサネットスイッチでは一旦ストアするため、入力した制御系フレーム長に依存した遅延が生じる。更に出力側で一般的な優先制御方法であるSP(Strict Priority)で転送すると、情報系フレームの転送中に制御系フレームが転送可能になっても、図1のように情報系フレームの転送を完了するまで制御系フレームの転送を開始できない。情報系フレームは比較的容量が大きく、例えば2,000バイトの情報系フレームの転送開始直後に制御系フ

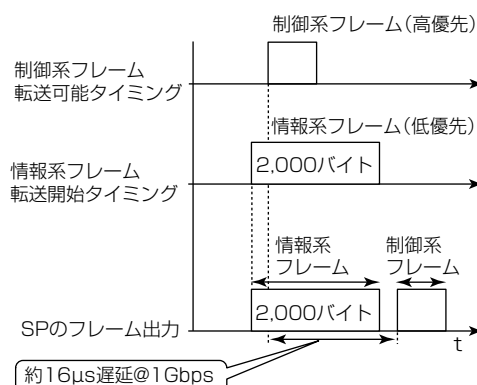


図1. SP方式

レームの転送要求が発生した場合、制御系フレームの遅延時間は、1 Gbpsの転送速度で約16 μ sとなる。

しかし、例えば工場内の作業ロボットの生産性を高めるために、制御系フレームのスイッチ1段の転送遅延を数 μ s以内に抑えたいという厳しい遅延要求を持つものもある。このように、制御系と情報系のトラフィックを同一ネットワークに収容するとき、従来転送方式では制御系トラフィックの遅延時間が増加し、その遅延要求を満足できないという課題がある。近年、これらの課題を解決するために、産業用のリアルタイム性が要求されるネットワークに必要なTSN技術の検討が加速している。3章では、これらのTSN技術の標準化動向について述べる。

- (注2) PROFIBUSとPROFINETは、プロフィバス協会の登録商標である。
 (注3) ControlNetは、ControlNet Internationalの登録商標である。
 (注4) INTERBUSは、フェニックスコンタクト株の登録商標である。
 (注5) EtherCATは、Beckhoff Automation GmbHの登録商標である。
 (注6) EtherNet/IPは、ODVAの登録商標である。

3. 標準化動向

2006年頃から規格化が開始されたEthernet AVB(IEEE 802.1AVB: Audio/Video Bridging)と呼ばれるEthernet経由で映像や音楽を伝送するための規格が策定され、主にEthernetの時刻同期(IEEE 802.1AS)とストリーム帯域予約(IEEE 802.1Qat)に関する規定がなされているが、一部の玄人向けのオーディオ・ビデオ配信のための規格であったため、広く普及していなかった。そこで、この規格の普及を推進するため、相互運用性を確保する適合試験を策定するAVnu Allianceを、Cisco社やIntel社が中心となり2009年に立ち上げた。これを2012年頃から産業界や自動車業界が着目し、産業用や車載用途に必要なリアルタイム性やフェイルセーフに関する議論が進められたことで、IEEE 802.1TSNの標準化が進められるようになった。そのため、TSNは当初Ethernet AVB Gen2と呼ばれていた。

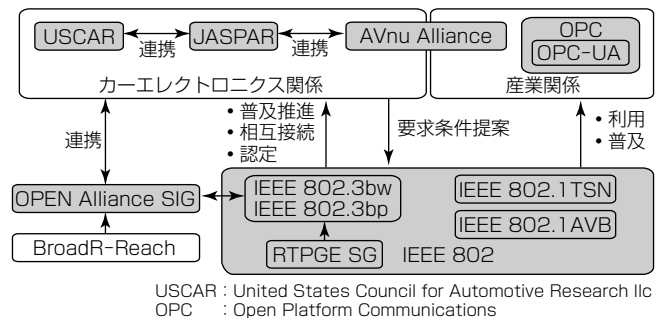
図2にIoTに向けた産業用イーサネットに関する規格化団体を示す。まず、日本では2004年に設立されたJASPAR(Japan Automotive Software Platform and Architecture)で、車載電子制御システムの高度化や複雑化に対し、特に車載

機器のソフトウェア化による開発費の増大が課題となっており、ソフトウェアやネットワークの標準化推進団体(AVnu AllianceやIEEE など)への車載要件の提案を中心に活動を行っている。

一方、イーサネットのリアルタイム性やフェイルセーフの向上とは関係はないが、車載のワイヤハーネスが乗用車1台で30kg前後にもなるとのことで、100Mbps又は1 Gbpsのイーサネットのシールドなし2線メタル伝送の物理層について、OPEN(One Pair Ethernet) Alliance SIGではIEEE 802.3bw(100BASE-T1)を推進し、RTPGE(Reduced Twisted Pair Gigabit Ethernet) Study Groupを得てIEEE 802.3bp(1000BASE-T1)の規格化が行われ、製品化が進められている。

また、工場等の産業界ではOPC-UA(OPC Unified Architecture)という異なるベンダーのオートメーション環境間の橋渡しをする標準化が進められており、そこではリアルタイム性を持たせるため、IEEE 802.1 TSNをレイヤ2以下の足回りの規格として利用する方向で議論が進められており、その状況は見逃せない。

以上を踏まえ、改めて表1に現在のIEEE 802.1TSNの規格化状況をまとめる。前述したように2012年頃から標準化が開始されており、4年目となる2016年には規格化完了が続々と進む状況となっているが、最近追加されたIEEE 802.1CMのように2019年5月に完了予定の規格もある。このIEEE 802.1CMはモバイルフロントホール向けにTSN技術を適用することで、低遅延の環境を提供することを目的に開始され、第5世代携帯基地局収容に向けて注目が集まっている。2016年に規格化完了予定のMAC層



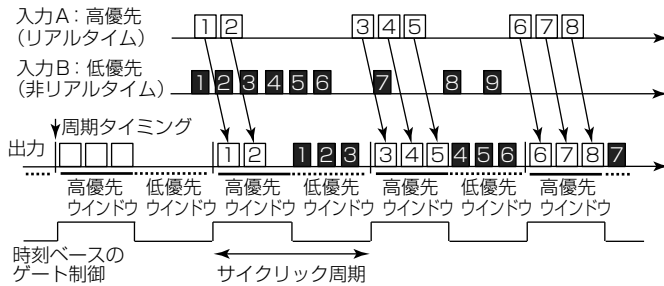


図3. IEEE 802.1Qbv

に近いところであるIEEE 802.1QbuやIEEE 802.1Qbvは、特に低遅延転送を実現する規格となっている。

リアルタイム性を実現する規格であるIEEE 802.1Qbvを図3に示す。規格の目的は、リアルタイムと非リアルタイムのトラフィックの混在収容とともに、周期的なリアルタイムトラフィックの伝送遅延を保証することにある。そのため、全てのノードや伝送装置との間で高精度な時刻同期を行い、サイクリック周期で、リアルタイムと非リアルタイムのトラフィックを時分割スケジューリングすることによって実現される。例えば入力Aのリアルタイムトラフィックは時刻を把握したノードから規定の時間で出力され、待つことなく高優先ウインドウで転送されるが、入力Bの非リアルタイムトラフィックは低優先ウインドウの時間まで待ってから出力されることとなる。

次にTSNで高信頼化を実現する規格であるIEEE 802.1CB (Seamless Redundancy)を図4に示す。他のTSNの規格より複雑であるため、少々遅れ気味であるが、目的を簡単に言うと、切替え時間を0sにすることであり、重要な制御フレームをロスさせないように複数経路にシーケンス番号とともにコピーして転送することで、途中で障害が発生しても他の経路の packets で目的のノードへ転送することができるという規格である。

最後にMACコントロール層の802.1Qbuから一部MAC層の部分であるとしてIEEE 802.3に変更されたIEEE 802.3br (IET: Interspersing Express Traffic)について述べる。この報告で試作検証した結果を後述するが、今までパケット単位での転送しか規定されていなかったが、パケットを分割して割り込ませる処理で高優先パケットの低遅延転送を可能とする。FP(Frame Preemption)方式とも呼ばれるこの方式は、低遅延転送を必要としない情報系フレームの転送中に低遅延転送が必要な制御系フレームの転送要求が発生した場合、図5に示すように、情報系フレームの転送を中断して分割し、制御系フレームを割り込み転送して、制御系フレームの遅延時間を低減する。IETでは、FPによって割り込むトラフィックの遅延時間を、1 Gbpsの転送速度でスイッチ1段で3 μ s以内に抑えることとしている⁽²⁾。割り込み転送によって分割(フラグメント化)された情報系フレームの未転送部分は、制御系フレーム転送完

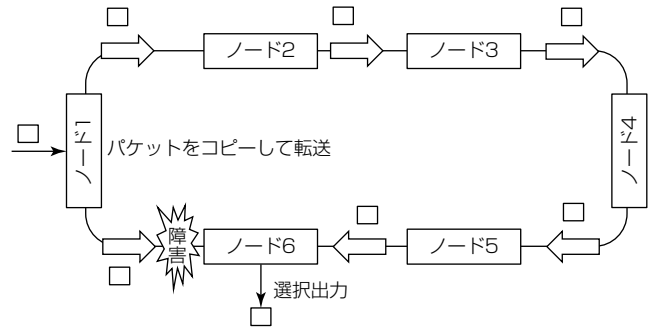


図4. IEEE 802.1CB

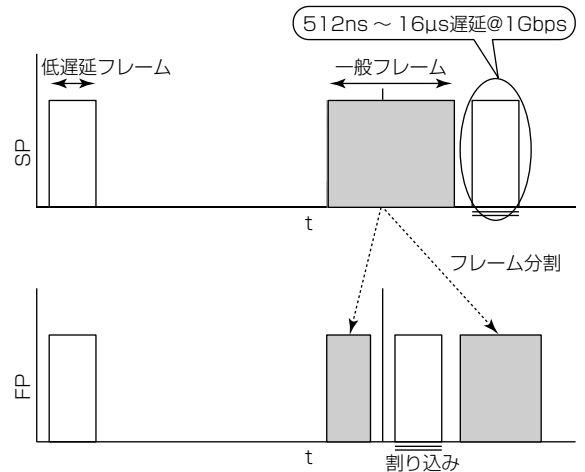


図5. IEEE 802.1br

了後に転送し、受信側のスイッチで結合して分割前のフレームに復元する。このため、フレームの再送・廃棄が発生せず、帯域を有効活用することができる⁽³⁾⁽⁴⁾。

以降、制御系で遅延要求の厳しいフレームをExpressフレーム、情報系で比較的遅延要求の厳しくないフレームをNormalフレームという。

4. 試作評価

試作では、IEEE 802.3brで標準化中のFP機能を備えたレイヤ2スイッチの基本機能を持つ1 Gbps \times 4ポートの低遅延イーサネットスイッチをFPGA(Field Programmable Gate Array)評価基板上に実装し、図6に示すスイッチ2段の評価系を構成し、Expressフレームの遅延時間の評価を行った。評価は、遅延時間の比較のため、図7のようにExpressフレームを高優先、Normalフレームを低優先とし、転送制御にFP方式を用いた場合と、従来のイーサネットでは一般的な優先制御方式であるSP方式を用いた場合の2通りで行った。

評価系ではイーサネットアナライザから出力されたExpress及びNormalフレームは、スイッチ#1のポート3及びポート4に入力され、スイッチで入力されたフレームが多重化されてポート1から出力される。次に、この多重トラフィックをスイッチ#2のポート1に入力させ、ス

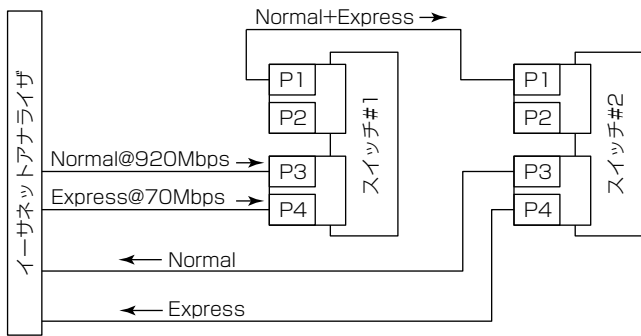


図6. 試作評価の構成

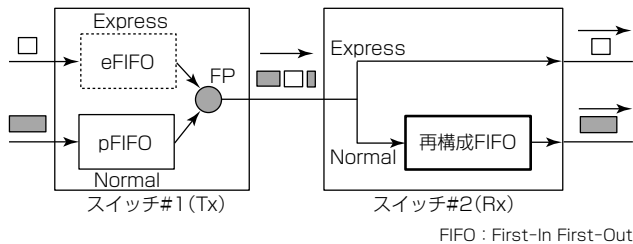


図7. FPによる割り込み転送

表2. データレート及びフレーム長

データ種別	データレート (Mbps)	フレーム長(バイト)
Express	70	128
Normal	920	64, 128, 256, 512, 1,024, 1,500, 2,000

表3. FP方式のExpressフレーム遅延測定結果

Normalフレーム長 (バイト)	Expressフレームの遅延時間(μs)			
	最大	最小	平均	揺らぎ
2,000	3.40	2.79	2.96	0.61
1,500	3.50	2.80	2.97	0.70
1,024	3.40	2.79	2.97	0.61
512	3.52	2.80	2.99	0.72
256	3.52	2.79	3.04	0.73
128	3.52	2.79	3.14	0.73
64	3.50	2.79	3.12	0.71

表4. SP方式のExpressフレーム遅延測定結果

Normalフレーム長 (バイト)	Expressフレームの遅延時間(μs)			
	最大	最小	平均	揺らぎ
2,000	22.90	6.52	14.26	16.38
1,500	18.51	5.66	12.07	12.85
1,024	14.32	5.69	9.87	8.63
512	9.82	5.26	7.52	4.57
256	7.57	5.22	6.36	2.35
128	6.44	5.22	5.79	1.22
64	5.89	5.22	5.51	0.67

スイッチ#2の内部で分離して、ポート3からExpressフレーム、ポート4から結合したNormalフレームを出力する。

Expressフレームの遅延測定は、アナライザから出力されたExpressフレームがスイッチ#1と#2を経由して、アナライザに戻るまでの遅延で行う。測定は、Normalフレームとの干渉による遅延の影響を検証するために、FP制御とSP制御のそれぞれの方式で、Normalフレーム長を

変化させながら、Expressフレームを10,000フレームずつ入力して行った。

表2は、測定におけるフレーム入力条件を示しており、Expressフレーム長は128バイトの固定で、データレートは70Mbpsである。一方、Expressフレームと競合するNormalフレーム長は、試行ごとに64バイトから2,000バイトの間で変化させ、データレートは920Mbpsとした。FP方式のスイッチとSP方式のスイッチをそれぞれ2段階ずつ通過したExpressフレームの遅延時間及び遅延揺らぎを表3、表4に示す。これらの結果から、このスイッチでFPを用いた場合の最大遅延時間は、Normalフレーム長によらず2段階で3.52μsであり、SP方式の場合は、Normalフレーム長が長くなるのに従って、最大22.90μsから大幅に改善し、Expressフレームの遅延揺らぎも低減されることが分かった。

5. む す び

IoT技術への関心の高まりによって注目されつつあるTSN技術の適用領域、課題、標準化動向について触れ、TSN規格群の1つでIEEE 802.3br IET Task Forceで標準化された転送方式を実装したイーサネットスイッチの低遅延転送性能の評価結果について述べた。

本稿で述べたTSN技術は、今後、工場内機器、列車、自動車等の産業用ネットワークの統一規格として普及する可能性があり、これらの標準技術を用いることで、従来技術では難しかった、アクチュエータ、センサ、コントローラ等で扱われる遅延に厳しい制御系トラフィックと、WebアクセスやEメール等の比較的遅延を許容する情報系トラフィックを同一伝送路上で多重化できるようになる。

参 考 文 献

- (1) Navet, N., et al.: Trends in automotive communication systems, Proc. of IEEE, **93**, No.6, 1204~1223 (2005)
- (2) Winkel, L.: Distinguished Minimum Latency Traffic, Joint IEEE -SA and ITU Workshop on Ethernet (2013)
http://www.IEEE802.org/3/DMLT/public/Jul13/ITU_IEEE_workshop_DMLT_Winkel_r0.pdf
- (3) IEEE 802.3br Interspersing express traffic Task Force (2015)
<http://www.IEEE802.org/3/br/index.html>
- (4) IEEE 802.3br Interspersing express traffic(IET) Task Force(TF) Baseline, ver1.0, rev.4 (2015)
http://www.IEEE802.org/3/br/Baseline/8023-IET-TF-1405_Winkel-iet-Baseline-r4.pdf

IoT時代のセキュリティ技術

米田 健*

Information Security Technologies in the Age of IoT

Takeshi Yoneda

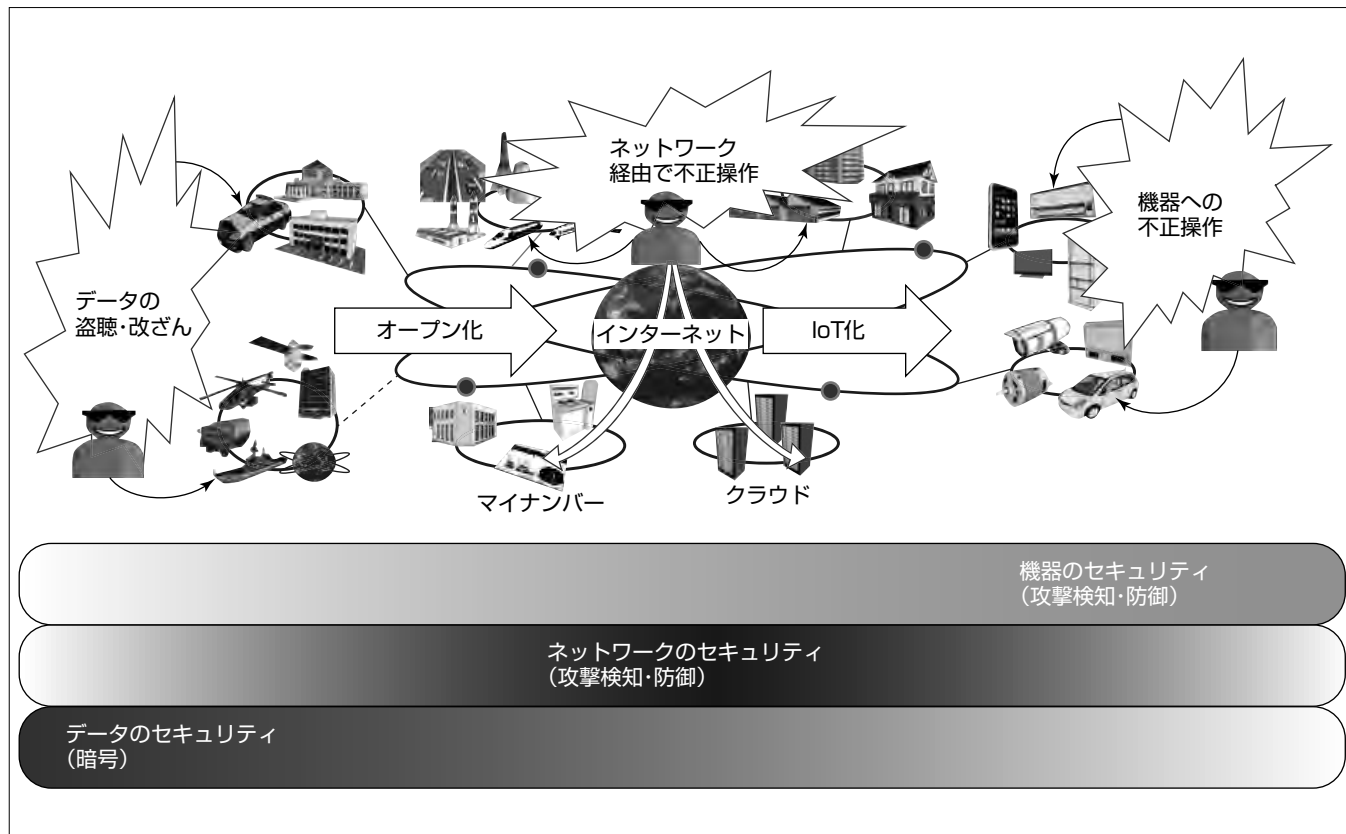
要 旨

近年、IoT(Internet of Things)の進展によってネットワークを介したサイバー攻撃による機密情報の漏洩(ろうえい)や重要インフラの機能不全のリスクが高まっている。また、米大統領が2015年9月の米中首脳会談で中国のサイバー攻撃に懸念を表明する等、サイバー攻撃は国家レベルの課題となった。日本政府もサイバーセキュリティ基本法を2015年1月に施行しサイバー攻撃対策への取組みを本格化した。そして、内閣に“サイバーセキュリティ戦略本部”を、内閣官房に“内閣サイバーセキュリティセンター(NISC)”を設置し、サイバーセキュリティ対策の立案・遂行を積極的に推進している。

サイバーセキュリティ対策では、データ、ネットワーク、機器のセキュリティが総合的に求められる。データのセキュリティは古くから防衛用途で盗聴・改ざん防止に活

用されてきた暗号が代表的である。一方、オープンなインターネットの普及・浸透に伴い、ネットワーク経由の情報システムに対する不正操作が深刻となり、それらを検知・防御するネットワークセキュリティも求められるようになった。そして、IoTの時代には、データとネットワークのセキュリティに加え、ネットワークにつながる機器への不正操作を防止する機器のセキュリティが重要となる。

三菱電機では、データ、ネットワーク、機器のセキュリティ技術として、データの秘匿と活用を両立させた秘匿検索技術、ネットワークを介したサイバー攻撃の手口に着目した攻撃検知・防御技術、機器に対する安全なソフトウェア更新や機器の認証を実現するLSIの指紋等の技術開発に取り組んでいる。



IoT時代のセキュリティ技術

2020年には500億台の機器がインターネットに接続されるとされており、データのセキュリティ、ネットワークのセキュリティに加えて、機器のセキュリティが重要となる。

1. ま え が き

近年、IoTの進展によってネットワークを介したサイバー攻撃による機密情報の漏洩や重要インフラの機能不全のリスクが高まっている。また、米大統領が2015年9月の米中首脳会談で中国のサイバー攻撃に懸念を表明する等、サイバー攻撃は国家レベルの課題となった。日本政府もサイバー攻撃対策への取組みを本格化するためのサイバーセキュリティ基本法を2015年1月に施行した。そして、内閣に“サイバーセキュリティ戦略本部”を、内閣官房に“内閣サイバーセキュリティセンター(NISC)”を設置し、サイバーセキュリティ対策の立案・遂行を積極的に推進している。

本稿では、IoT時代の安全・安心の要となるサイバーセキュリティへの日本政府の取組みと当社の取組みを述べる。また、当社のサイバーセキュリティの研究開発への取組みとして、データのセキュリティ、ネットワークのセキュリティ、機器のセキュリティの差別化技術について述べる。

2. 日本政府の取組み

2015年9月4日に内閣で閣議決定された“サイバーセキュリティ戦略”⁽¹⁾では、経済社会の活力の向上及び持続的発展のために、IoTシステムのセキュリティ確保が必要であることを強調している。また、国民が安全で安心して暮らせる社会の実現のために、重要インフラのセキュリティ確保が必要であることを強調している。

取組みを強化する施策として、①効率のかつ迅速な官民のサイバー攻撃情報の共有、サイバー攻撃を検知・防御する組織の構築と組織間の連携、②機器・システムの開発・運用プロセスのセキュリティ基準・ガイドライン策定・遵守促進、③第三者認証によって客観的に機器・システムや組織のセキュリティを評価・認証する制度の確立が挙げられている。また、これらの組織、開発・運用プロセス、制度の観点からのセキュリティへの取組み強化に加え、研究開発の観点から、暗号のようなコア技術、サイバー攻撃の検知・防御技術への取組みが強化されている。

3. 当社の取組み

当社では、サイバー攻撃情報の共有窓口となるCSIRT(Computer Security Incident Response Team)の設置、官民CSIRT間の情報共有等連携を目的とした日本シースアート協議会等の団体への参加を通じて、官民との連携を意識したセキュリティ組織の構築に取り組んでいる。また、技術研究組合 制御システムセキュリティセンター(CSSC)に参画し、制御システムの汎用的なセキュリティ標準として注目されるIEC62443をベースとしたセキュリティ評価・認証手法や開発・運用プロセスのセキュリティガイドラインの調査・研究に取り組んでいる。

また、差別化技術としては、データセキュリティ、ネットワークセキュリティ、機器セキュリティの各分野でIoT時代のニーズを先取りした研究開発に取り組んでいる。

4. データのセキュリティ：秘匿検索

4.1 開発の背景

IoTの時代には、人や機器の情報をクラウドに収集して分析するビッグデータ処理によって、付加価値創出が期待される。しかし、人や機器の情報は、機密性が高くクラウドに保存する場合には暗号化が求められる。一方、従来、暗号化された情報を検索する場合、一旦クラウドで復号する必要がある、その際に機密情報が漏洩する懸念があった(図1)。そこで、クラウドで復号することなく検索できる暗号“秘匿検索”技術を開発した。この技術によって、情報の秘匿と活用の両立を実現できる。

4.2 秘匿検索の仕組み

秘匿検索の実現には、暗号化された検索要求とクラウドに登録された暗号化データの一致・不一致をクラウドで判定する演算が必要となる。その演算を2010年にNTTと共同開発した内積述語暗号⁽²⁾に基づいて実現した。

(1) 内積述語暗号

内積述語暗号を用いると、2つのベクトルを暗号化したまま内積を計算し、ベクトルが直交していれば(内積が0ならば)0、それ以外ならば乱数を返す関数 f を実現できる。具体的には、図2に示すように、公開鍵(pk)で暗号化(E_{pk})したベクトルと秘密鍵(sk)で暗号化(E_{sk})したベクトルの内積を計算すると、暗号化前のベクトルが直交している場合0、直交していない場合は乱数が結果として得られる。

(2) 登録データと検索キーワードのベクトル符号化

内積述語暗号のベクトル直交性判定を、秘匿検索に応用するために、登録するデータと検索キーワードのベクトル符号化手法を開発した。具体的には、登録するデータと検索キーワードが一致した場合に直交する(内積が0となる)ようにベクトル符号化する。図3では、“吉田”というデー

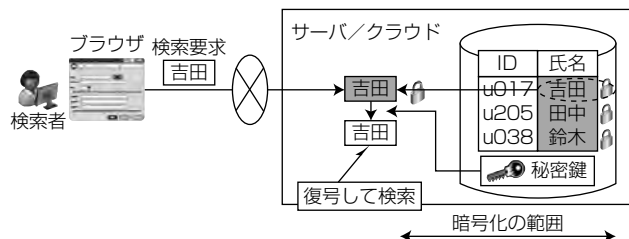


図1. 従来の暗号化データの検索

$$E_{pk}(\vec{a}): \vec{a} \text{ の公開鍵による暗号化}$$

$$E_{sk}(\vec{b}): \vec{b} \text{ の秘密鍵による暗号化}$$

$$E_{pk}(\vec{a}) \cdot E_{sk}(\vec{b}) = f(\vec{a} \cdot \vec{b}) = \begin{cases} 0 & \vec{a} \cdot \vec{b} = 0 \text{ の場合} \\ \text{乱数} & \vec{a} \cdot \vec{b} \neq 0 \text{ の場合} \end{cases}$$

図2. 内積述語暗号を用いたベクトルの直交性判定

タを、登録データ及び検索キーワードにする場合のベクトル符号化例を示す。

このベクトル符号化によって、サーバは、暗号化された登録データと暗号化された検索キーワードをそのままベクトル直交性判定し、結果が0であれば、登録データと検索キーワードが一致していることが分かる(図4)。

このような秘匿検索によってクラウドは、暗号化された検索要求とサーバに登録された暗号化データの一致・不一致を一切復号することなく判定でき、情報漏洩の懸念を払拭することができる。

4.3 秘匿検索の発展

(1) 部分一致対応型秘匿検索

インターネットの検索エンジンを利用する場合、キーワードをブラウザから入力すると、そのキーワードを含むホームページやドキュメントが検索結果として表示される。このような“キーワードを含むドキュメントの検索”を暗号化したまま実施するためには、4.2節で述べた秘匿検索では不十分である。なぜなら、登録データと検索キーワードが完全に一致しているかの判定は実現できているが、登録データに検索キーワードが含まれること、つまり、部分一致判定は暗号化したまま実現できていないからである。

そこで、2016年2月に部分一致を暗号化したまま判定できる部分一致対応型の秘匿検索基盤ソフトウェアを世界で初めて(注1)開発した(3)(図5)。

(注1) 2016年2月4日現在、当社調べ

(2) 部分一致対応型の秘匿検索の仕組み

部分一致対応型秘匿検索では、登録データのある位置に、検索キーワードが存在することを暗号化したまま判定するために、各文字が先頭から何文字目の位置にあるかを表す“文字位置”の情報を各文字の暗号化と同時に埋め込む技術と、埋め込まれた“文字位置”を暗号化したままスライドさせる技術を実現した(4)(図6)。これらの技術を4.2節のベクトル符号化と組み合わせることによって、暗号化された検索キーワードに埋め込んだ“文字位置”をスライドさ

せ、暗号化された登録データの対応する位置に一致する文字列が存在するかを判定できる。なお、一致判定には、4.2節(1)で述べた内積述語暗号を用いている。

4.4 今後の取組み

部分一致対応の秘匿検索の実現によって、秘匿検索の適用範囲を、機器の稼働ログやネットワークの通信ログ等の定型データから、オフィス文書や医療文書等の非定型データに広げることが可能となった。今後は適用分野に応じた最適化に取り組む。

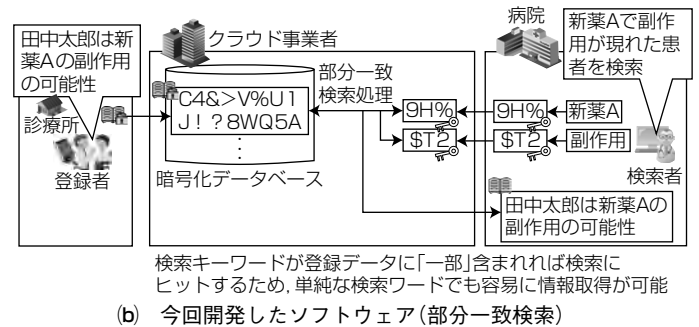
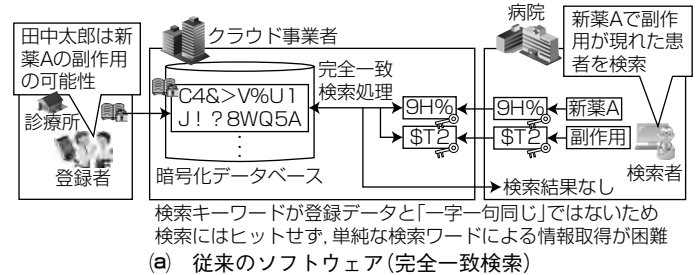


図5. 部分一致対応型秘匿検索

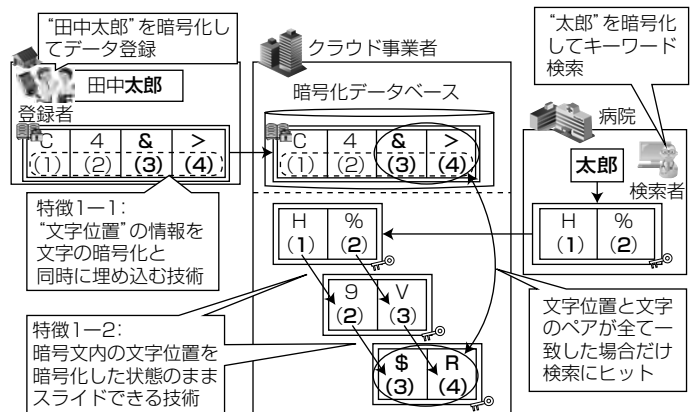


図6. 暗号化したまま文字位置のスライド

登録データ $\bar{a} = (\text{吉田}, 1)$
検索キーワード $\bar{b} = (-1, \text{吉田})$ ($\bar{a} \cdot \bar{b} = \text{吉田} * -1 + 1 * \text{吉田} = 0$)

図3. 登録データと検索キーワードのベクトル符号化例

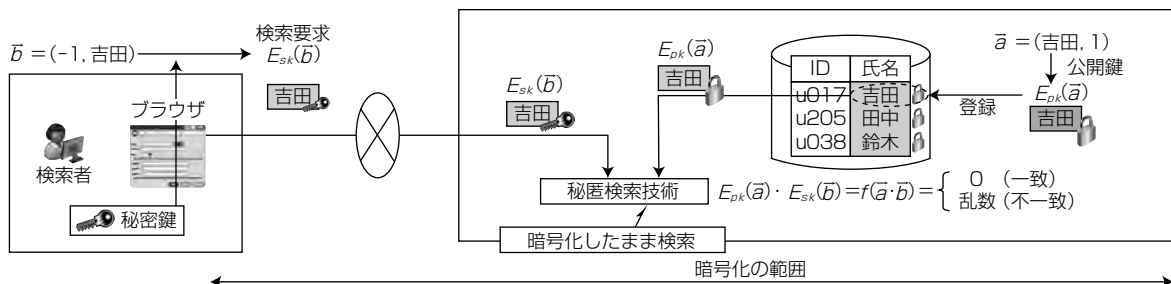


図4. 内積述語暗号を用いた秘匿検索

5. ネットワークのセキュリティ：攻撃検知技術

5.1 開発の背景

近年、企業や政府・自治体で発生する大規模情報漏洩は、ウイルスが添付されたメールや、ウイルスが仕込まれた不正なWebサイトを用いたサイバー攻撃によってもたらされる。ウイルスは年間3億種の新種が発生しており、過去のウイルスと一致するウイルスを見つける手法では検知が困難となっている⁽⁵⁾。

この課題を解決するため、個々のウイルスではなく、ウイルスを用いた攻撃者の手口に着目して攻撃を検知する方式を開発した。分析の結果、攻撃者の手口は50程度であることを解明し、手口に着目することで効率的な攻撃検知を実現した⁽⁶⁾。

5.2 手口に着目した攻撃検知の仕組み

サイバー攻撃におけるウイルスの活動は、攻撃対象の端末に感染、ハッカーからの指示を受信、感染端末を調査し、さらに活動を広げるため不正にアクセス権を入手するという段階を踏む。例えば、感染端末を調査する活動段階では、感染端末に保存されているドキュメントの検索、通信ルートの確認、セキュリティ対策設定の確認という複数の攻撃手口によって、何をどのように盗み出すかを決定する。

そこで、ウイルスを用いた共通の攻撃手口を50個程度に分類し、各攻撃手口の発生をログから検知する分析ルールを開発した。攻撃手口の増加は、1年で10数件程度であり、新しい攻撃手口が確認された段階で分析ルールを追加することが可能となる。

また、正規ユーザーの活動が、攻撃手口と類似している場合、その活動が、攻撃ではないことを判断する必要がある。そこで、この攻撃手口をいくつか連続させたサイバー攻撃シナリオを定義し、攻撃手口が、攻撃シナリオに沿って発生しているかをチェックする相関分析手法を開発した。この手法によって、攻撃手口に類似した正規ユーザーの活動とサイバー攻撃との識別が可能となる(図7)。

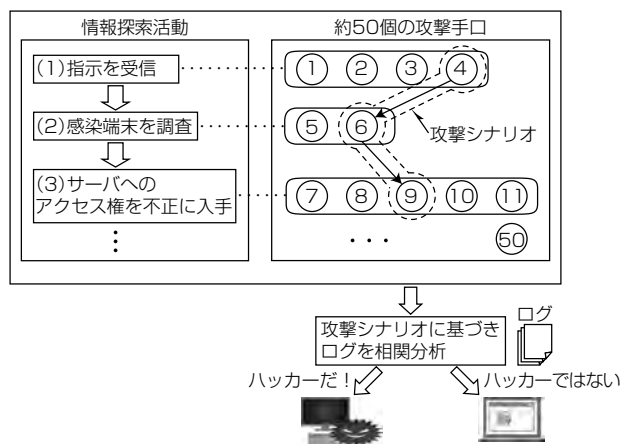


図7. 攻撃シナリオに基づくサイバー攻撃検知

5.3 今後の取り組み

この技術は、情報システムに対する攻撃を対象として開発した。一方、IoTシステムに対する攻撃でも、攻撃者は共通の限定的な攻撃手口を用いると予想される。そこで、この技術の適用範囲をIoTシステムに対する攻撃に拡張するために、機器への攻撃手口の調査・分析に取り組む。

6. 機器のセキュリティ：LSIの指紋

6.1 開発の背景

パソコンやスマートフォン等の情報通信機器だけでなく、あらゆる機器がインターネットを介してつながるIoT時代が本格化している。“つながる”ことで利便性が向上する一方で、セキュリティリスクとして不正プログラムの混入やなりすまし等の対策が求められている。従来のリスクは銀行の不正送金等仮想社会での被害であったのに対して、IoTでは機器を含め様々なシステムとつながり、被害にあえば直接人命に関わる場合もある。

一般的に電子機器はLSI(大規模集積回路)に組み込まれたプログラムによって機器の動作が制御されている。もしそのプログラムが改ざんされれば、ネットワークにつながる全ての機器に危険が及ぶ。これらの課題の解決を目指して開発したのがLSIの指紋⁽⁷⁾⁽⁸⁾である。

6.2 LSIの指紋の仕組み

機器には、機器の制御を行うプログラムと、それを実行するCPU等のLSIが搭載されている。LSIは同じ回路であっても個体差によって、同じ出力でも個体ごとに過渡状態での電圧上昇パターン“グリッチ”が異なる。これを利用してLSIの指紋とも言える固有IDを生成する。

LSIの中の秘密情報を守るには条件が2つある。まず1つは“LSIを分解・解析しても情報が漏れないこと”である。これまでID情報は暗号化した上で、不揮発性メモリ(電力供給がなくてもデータを保持できる記憶素子)に格納するのが一般的であった。しかしこれでは分解・解析することでメモリの情報を盗み見られる可能性がある。この技術では固有IDはLSIが動作しているときにしか現れず、仮に分解しても秘密情報はどこにも存在しない。もう1つの条件は“回路が複製されても秘密情報を複製できない”ということである。“グリッチ”の違いは不規則な個体差によって発生する。つまり回路を複製しても、同じIDにはなりえない。“見えないID・複製できないID”という安全性を証明する2つ条件をこの技術はクリアした。

6.3 固有IDの生成方法

LSIに対する信号の入力によって最終的な出力の信号が安定するまでの過程で、電圧の上昇が個体ごとに異なる現象を利用して固有IDを生成する(図8)。

①信号を入力すると発生する電圧の上昇パターン(“グリッチ”)の回数を数え、その数が偶数個ならば0、奇

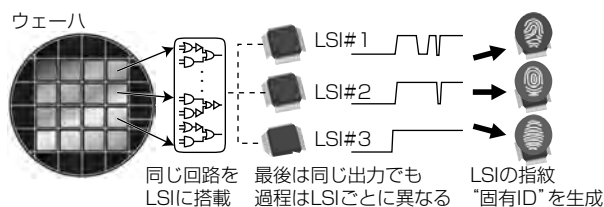


図8. LSIの指紋の仕組み

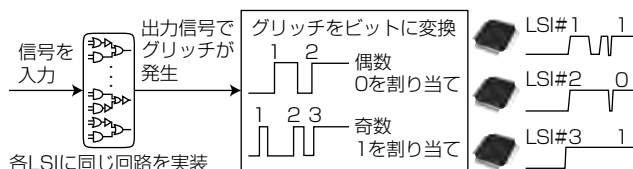


図9. 固有IDの生成方法

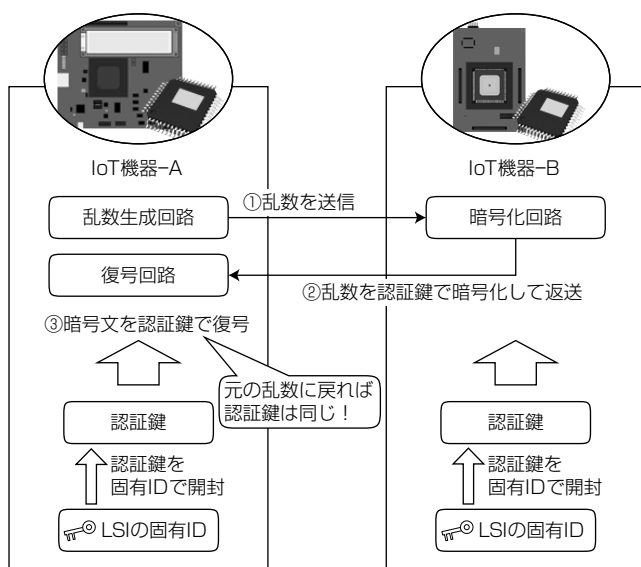


図10. 相手認証の仕組み

数個ならば1のビットを与える。

②入力する信号を変えて繰り返しビットに変換し、指紋のような固有ID情報を生成する(図9)。

6.4 危険なプログラム混入や不正アクセスの防止

固有IDを利用すれば、機器に対する危険なプログラムの混入等を防ぐことができる。例えばインターネットを介して機器にプログラムを送る際、LSIの固有IDで復号できるように暗号化してプログラムを送信する。もし固有IDで復号できないプログラムが送られてくれば、不正なプログラムと見なし動作を拒否することで、悪意ある攻撃から機器を守る。

もう1つの利用方法は認証鍵を用いた相手認証である(図10)。認証鍵は製造メーカー等が独自に設定するもので、機器の信頼性を証明する。接続する機器同士は互いの

認証鍵を使って乱数を暗号・復号しあうことで相手の認証鍵を確認し、同じ認証鍵を持つ機器同士であれば接続を許可する。この手法で大切なのは認証鍵である。もし漏れれば、不正な接続を許すことになる。そこで認証鍵をそのまま格納するのではなく、固有IDで暗号化して格納する。

6.5 今後の取組み

IoT時代における組み込み機器のセキュリティリスクに対して、LSIの固有IDを応用したプログラム保護や機器のなりすまし防止によって、コストを抑えつつ組み込み機器の安心・安全に貢献することが可能となる。この技術の適用を当社製品機器から拡大していく。

7. む す び

IoTシステムのセキュリティ向上には、製品・システムを提供する企業がセキュリティ対策を適切に実装することが求められる。企業によるセキュリティ実装促進のためには、どのような脅威に対して、どこまで対策をとればよいのかというコンセンサスを業界ごとに確立することが重要である。

今回述べたような差別化技術の研究開発に加えて、業界ごとのセキュリティ対策のコンセンサス作りにも積極的に参画し、IoT時代の安全・安心社会の実現に貢献していく。

参 考 文 献

- (1) <http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-c.pdf>
- (2) Okamoto, T., et al.: Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, CRYPTO, 191~208 (2010)
- (3) <http://www.mitsubishielectric.co.jp/news/2016/0204.html>
- (4) Kawai, Y., et al.: SEPM: Efficient Partial Key word Search on Encrypted Data, CANS, 75~91 (2015)
- (5) シマンテック社: 2015年インターネットセキュリティ脅威レポート
- (6) <http://www.mitsubishielectric.co.jp/news/2016/pdf/0217-f.pdf>
- (7) Suzuki, D., et al.: The Glitch PUF: A New Delay-PUF Architecture Exploiting Glitch Shapes, CHES (2010)
- (8) <http://www.mitsubishielectric.co.jp/news/2015/0205.pdf>

設備維持管理向けデータ分析技術

平井規郎* 栗山俊通*
中村隆顕* 上田宜史*
増崎隆彦**

Data Analysis Technologies for Maintenance and Management of Facilities

Norio Hirai, Takaaki Nakamura, Takahiko Masuzaki, Toshiyuki Kuriyama, Takafumi Ueda

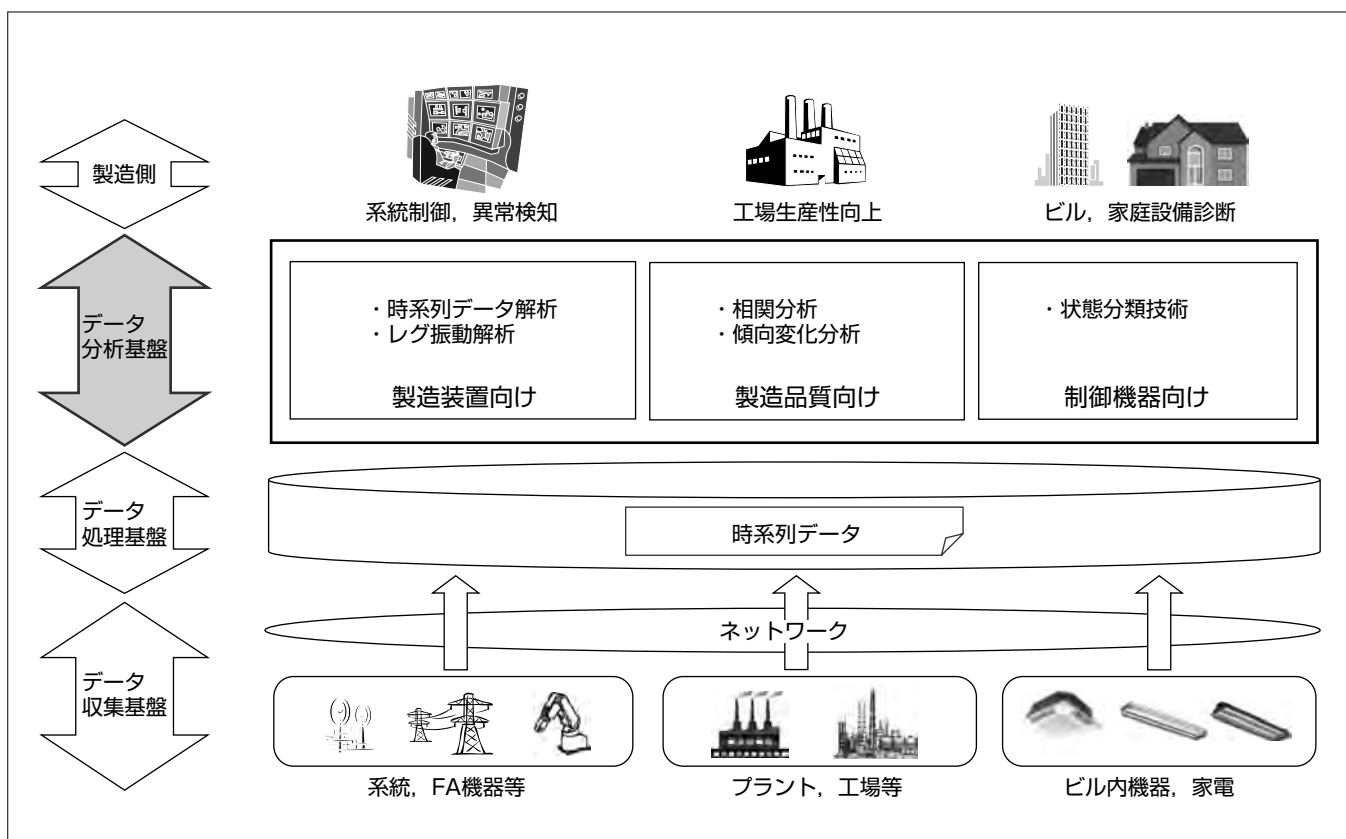
要 旨

近年、IoT(Internet of Things)の普及によって、大量の機器がネットワークに接続され、様々な機器のセンサデータを収集することが可能になってきた。それに伴い、機器の状態を遠隔から監視するだけでなく、データを分析し、機器の将来の状態を予測することで、予防保全や製造品質維持への活用が期待されている。

予防保全への活用では、設備が故障する前にセンサデータから故障の予兆を検知し、故障発生前の保全を可能にすることで製造ラインのダウンタイムを削減し、効率的な保守を可能にする故障予兆検知技術や、故障が発生した場合に故障要因の候補を提示することで効果的な保全を可能にする要因分析技術などがある。一方、製造品質維持への活

用では、製造ラインの検査設備などにおけるデータの傾向変化と不具合製品との関係を分析し、不具合製品の製造を未然に防止することを目的とする傾向変化分析や、検査基準を最適化し歩留向上を目的とする検査基準最適化がある。

これらを実現する分析技術は多様であるが、分析対象によってデータの前処理やモデル化が大きく異なることが分かっている。そこでまず、分析対象を製造装置、製造品質、制御機器の3つの分野に分け、それぞれに適した分析技術を開発した。一方、分析効率化という観点から、分析技術の共通部分を統合し、多様な分析対象に対してカスタマイズを軽減することで分析を効率化するデータ分析基盤を開発した。



予防保全システムへの故障予兆検知技術の適用例

予防保全システムに故障予兆検知技術を適用することで、機器や装置が故障に至り停止する前に対策をたてることが可能になり、ダウンタイムゼロを実現し、効率的なメンテナンスプランを立案することができる。例えば、ある機器がシステム全体の一部として稼働している場合、機器の異常を早期に検知することで、他の機器のメンテナンスと時期を合わせてメンテナンスし、生産性を向上させることが可能になる。

1. ま え が き

近年IoTの普及に伴い、設備の異常検知や故障予測によって、故障発生前にメンテナンスを行うことでダウンタイムの削減を可能にする予防保全や、不具合製造を未然に防止して品質を向上させる取組みが行われている。三菱電機も、設備の状態をデータから推定及び予測し、故障が起きる予兆を検知することで故障の発生時期を予測する技術や、検査データから傾向変化や検査基準を分析して品質を向上させる品質分析技術の開発に取り組んでいる。

本稿ではこれらのデータ分析技術について述べる。

2. 設備維持管理向けデータ分析技術

設備維持管理に向けたデータ分析技術には、設備や装置が故障する前に、センサデータから故障の予兆となる異常を検知する故障予兆検知技術や、製造ライン上で検査設備のデータを分析し、不具合製品が製造される前に兆候を検知する品質分析技術などがある。故障予兆検知の場合、通報を受けた制御システムは、該当の装置を安全に停止させることができる。また、現場作業者が該当の装置をチェックし、保守員が知識や経験から故障直前と判断した場合は、装置を交換・修理する。故障予兆検知の主要な効果は次の3つである。

- (1) 製造工程では、材料や部品を製造装置に投入する前に、装置を停止させることで、材料や部品のロスを削減することができる。
- (2) 小さな故障がより大きな故障に発展する前に、対策をとることが可能になり、重大な故障が発生した場合に必要な対策コスト(人手、時間)を削減することができる。
- (3) インフラ設備では、提供するサービスの停止時間を削減することができる。

データ分析はこれらを実現するための手段である。データを分析するためには一般的に、要求分析に基づく目標設定を行った後は、データ処理を適切に進めるためのデータ

の性質理解、データのモデリング、モデルの評価、運用という手順で進めていく。データ分析を成功に導くためには、これらの手順の中でも最初の“センサ要件定義”と“故障予兆モデル生成”(図1)が重要である。

しかしデータの“性質理解”と“モデリング”は分析対象ごとに異なるため、汎用化が困難である。そこで、本稿では分析対象を製造装置、製造品質、制御機器に分類し、それぞれの特性を考慮したデータ分析技術開発の取組みについて述べる。一方、これらの分析技術の共通化できる部分を統合することで、分析技術開発を効率化するための分析基盤技術開発の取組みについても述べる。

3. 製造装置向けデータ分析技術

ここでは、製造装置の故障予兆検知のためのデータ分析技術について述べる。製造装置が導入されている製造工場で、稼働中に故障・停止すると、損害額が大きくなる(数千万円規模)場合がある。そのような現場では故障の予兆検知のニーズが大きい。そこでこのような装置での故障直前の温度や電流データから、通常と異なるデータの変化を検知することで故障予兆を検知する技術を開発した。この技術は、時系列データの時間的変化の微小な差異を検出可能にする。これによって、時系列データを収集することが可能な製造装置について故障の予兆検知が可能になる。

3.1 時系列データ解析技術

製造ラインの装置では、装置の保全のために、装置から収集される複数の信号から、故障予兆に関連する異常を検知したいというニーズがある。一般的に製造装置では大きな障害は通常発生しないことから、“学習のための異常データがなくても異常検知ができなければならない”という要請がある。また、従来の多くの異常検知アルゴリズムは、必要とするパラメータが多くて使いこなすのが難しいという課題がある。一方、“製造ラインの装置には温度、熱量、圧力、振動、電圧などの様々な特性を持つ多様かつ多数の信号があるため、信号の特性ごとにチューニングする

手間を不要にしたい”という要請がある。このようなニーズを満たす技術としては、与えられた時系列データから通常と異なる部分列を発見するアルゴリズムDiscord方式⁽¹⁾がある。Discord方式は、次の手順で異常を検知する。

- (1) 異常でないと仮定されるデータ(学習データ)と、異常検知の対象となるデータ(テストデータ)を準備する。
- (2) 学習データから与えられたサイズの部分列を全て作成する。
- (3) テストデータについても同様に全ての部分列を作成する。
- (4) テストデータの部分列と学習データの部分列

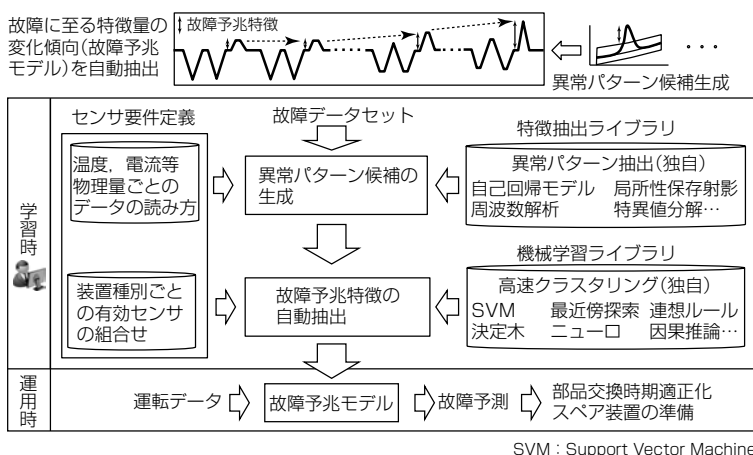


図1. 故障予兆モデリングの流れ

との距離を総当たりで計算し、計算された距離の中で、最も小さい距離を基準として異常の度合いを定義する。

すなわち、学習データ中の全ての部分列と似ていないテストデータの部分列を異常な部分列として抽出するため、わずかな差異に対しても高精度に検出することが可能であるが、一方で異常検知に要する時間が学習データの長さに比例するという課題がある。

これに対し、学習データ中の部分列の中から典型的な特徴を持つ部分列(以下“標本部分列”という。)を選択し、総当たりでなく標本部分列とだけ距離を比較することによって、従来の総当たりの手法よりも40倍程度高速に異常な部分列を検索することで、リアルタイムに異常を検知することを可能にする方式を開発した。図2に異常検知結果の例を示す。これらの2つの例では、周期的に変化するデータに含まれる、通常とは異なる挙動(丸枠部)が検知できていることが分かる。

3.2 レグ振動解析技術

製造装置の保全業務では故障予兆や劣化を検出するため、不規則に変動するセンサ時系列に対して、与えられた振幅を超える上下変動の頻度を算出したいというニーズがある。上下変動の例を示す。

例1：空調機で、正常時は、部屋の実測温度はある一定時間後に設定温度に収束するが、センサや制御系に異常がある場合には、設定温度より高い温度と低い温度の間を振動する(ハンチング現象)。

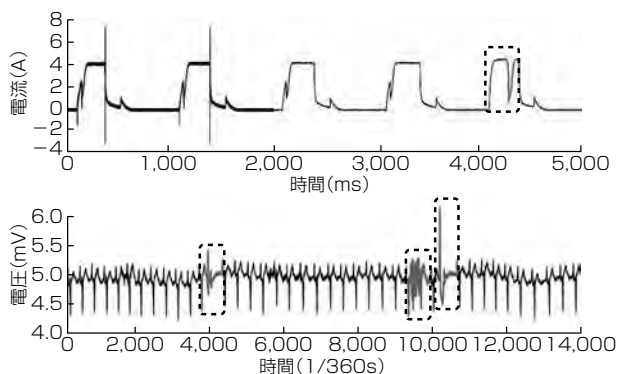


図2. 異常検知技術による検知例

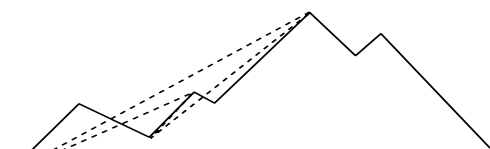


図3. レグの概念図

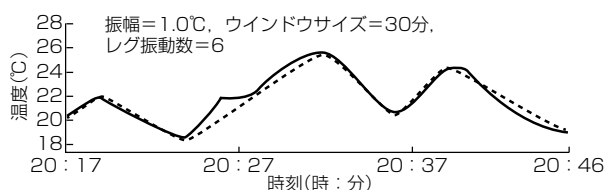


図4. レグを用いた振動解析

例2：配管詰まりがある場合の圧力の急激な上昇・下降不規則に変動する時系列の上下変動を扱った従来技術として、データ工学分野ではレグがある。レグは、図3の点線に示すように、不規則な上下変動があっても全体として上昇、ないし下降している部分列のことを言う。

従来技術は、単独のレグによって上昇/下降傾向の異常を検知するため、例に示すような上下変動を検知することができなかった。そこで、上昇傾向と下降傾向のレグが交替出現するレグ振動を高速に検知するレグ振動解析技術を開発した。レグ振動解析技術を利用することで、図4に示すように、“30分間に温度が1℃以上の幅で4回以上振動したら異常”といった複雑な条件で異常を検知することが可能になった。

4. 製造品質向けデータ分析技術

製造ラインにおける歩留向上や製造原価の低減を目的とした製造データ分析として品質分析がある。例えばQC 7つ道具(パレート図、特性要因図、管理図含めたグラフ、チェックシート、ヒストグラム、散布図、層別)を用いて、情報を正しく分析し、品質改善活動を行ってきた。しかし、これらの手法は問題が発生した後に、問題の発見、原因把握、解消確認を行うためのものであり、品質問題の発生を予測することは困難であった。そこで、品質向上、問題発生予測を目的として、次の2つの技術を開発した。

- (1) 工程間に存在する関係性に基づく製造品質の向上を目的とする相関分析技術
 - (2) データ特性の傾向変化と不具合の関係に基づく不具合製造の未然防止を目的とする傾向変化分析技術
- 次にこれらの技術について述べる。

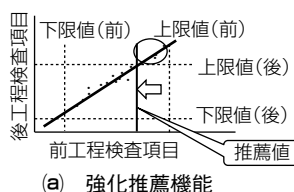
4.1 相関分析技術

検査工程間の製造データに相関がある場合、ある工程の可否を判定するための検査基準値を変化させることによる後工程への影響を把握することができる。そこで、検査間の相関分析によって、最適な検査基準値を求めるため、“強化推薦機能”と“緩和推薦機能”の2つの機能を開発した。

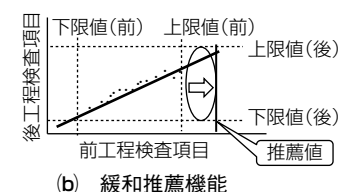
“強化推薦機能”は、基準値の強化によって、後工程での不合格の削減を目標としている。一方“緩和推薦機能”は、基準値の緩和によって、前工程での不必要な不合格の削減を目標としている(図5)。

基準値強化によって後工程の不合格を削減できる前工程の検査項目
 ⇒品質安定化

基準値を緩和しても後工程に影響を与えない前工程の検査項目
 ⇒原価低減、歩留向上



(a) 強化推薦機能



(b) 緩和推薦機能

図5. 相関分析による2つの機能

4.2 傾向変化分析技術

製造時期や、保守・点検などのイベントによる製造データ特性の傾向変化を求めることで、検査における不合格発生頻度増加等の不具合に寄与する条件を抽出する。これによって、条件やイベントごとに、不具合増加の未然防止策を検討することができる。

この技術は、不合格発生頻度や、製造データの時系列的な変化量、任意の検査項目の測定値をロット名・製造時期・製品仕様といった条件で抽出した頻度分布を、別の条件で抽出した頻度分布と比較することで、様々な条件による製造データの分布の差異確認を可能とする。製造時期や保守・点検などのイベントによる検査データの傾向や不合格の頻度を確認することで、時期ごとの傾向に応じた検査基準値の厳格化や不合格発生頻度増加の兆候発見による不具合製品製造の未然防止ができる(図6)。

5. 制御機器向けデータ分析技術

機器の運転に周期性がなく、かつ運転状態の変化が激しい制御機器では、物理モデルから推定される異常の検知精度が低下してしまう、という課題がある。これに対して従来は発停前後や、センサデータの振幅が大きいなどの制御が不安定な過渡状態のデータを取り除くことで、検知精度を向上させていた。しかしこのようなルールベースにおける前処理だけでは、制御機器の内部で複雑な制御を行っている場合、多様な運転状態が含まれるため異常検知結果のばらつきが大きい。そこで、物理モデルと統計モデルとを併用した前処理を行うことで、異常検知精度を従来の精度からさらに向上させる状態分類技術を開発した。

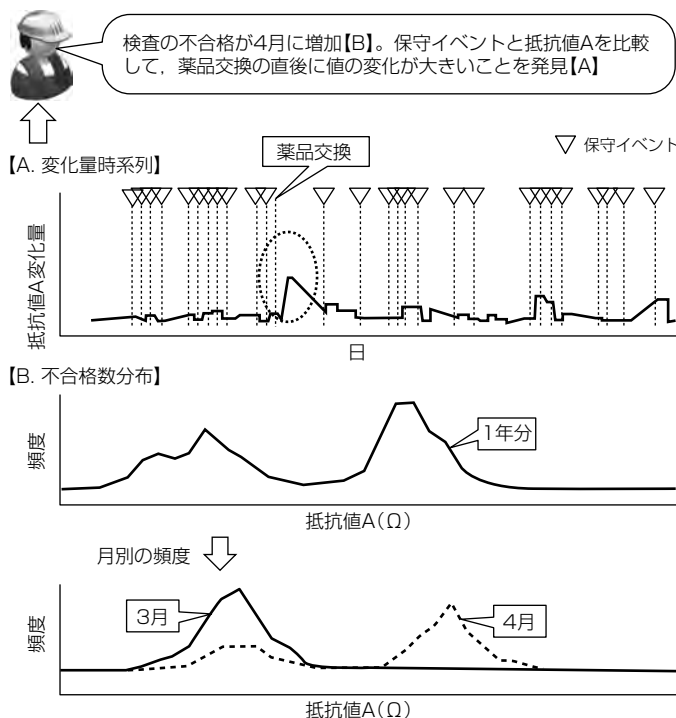


図6. 傾向変化分析

先に述べたとおり、機器の設置環境の影響や、機器内部の複雑な制御によって、制御機器では様々な運転状態が発生する。その結果、誤検知を防ぐため、異常検知のしきい値を緩和せざるを得ず、十分な精度が得られない。そこで、高精度な異常検知実現のためには、機器データを運転状態ごとに分類し、同じ運転状態でデータを分析する必要がある。運転状態を分類する1つの手法として、各センサデータの値域を等間隔に分割し、その組合せを1つの運転状態とする方式が考えられる。しかし、近年は、センサ数も膨大であり、この方式は現実的とは言えない。そこで、制御機器で収集される多次元のデータを、その特徴を反映して次元を圧縮する統計手法である特異値分解(Singular Value Decomposition: SVD)を利用し、データを一次元に圧縮し、分割する方式を検討した。特異値分解では、多次元データに対し、最もデータの特徴を示す特徴空間を抽出することが可能である(図7)。

具体的には、特徴ベクトル U は、式(2)を満たす重み l_i を利用し、式(1)に示すように、各センサ項目の一次結合によって求められる。特異値分解では、 U の分散が最大となる l_i の固有値問題を解くことによって求めることができる。

$$U = l_1 x_1 + l_2 x_2 + \dots + l_n x_n \dots \dots \dots (1)$$

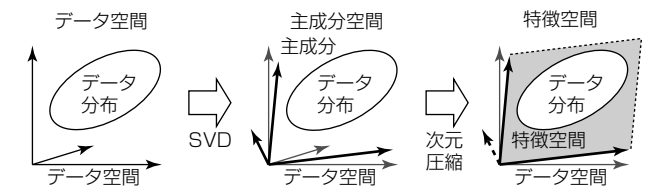
$$l_1^2 + l_2^2 + \dots + l_n^2 = 1 \dots \dots \dots (2)$$

l_i : センサ i の重み

x_i : センサ i の計測値(ベクトル)

図8に示すとおり、多次元データの特徴を反映する特徴空間を形成する軸(特徴ベクトル U)上で、データをクラス

特異値分解(SVD)を用いることで、データの特徴をよく反映する軸(主成分)を算出できる。



主成分は、元データの項目の特性を集約したものであるため、主成分値を評価することで、複数の値にわたる変動の特性についても評価することができる。

図7. 特異値分解

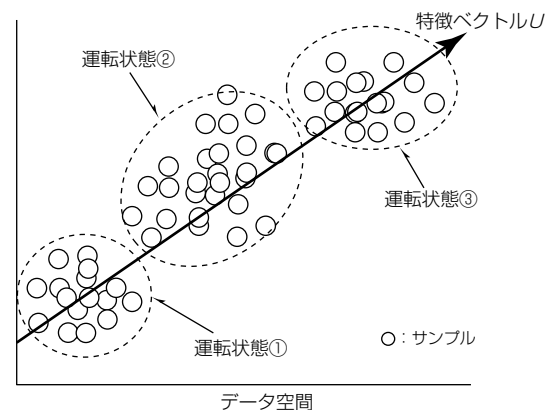


図8. ベクトル上におけるクラスタリング

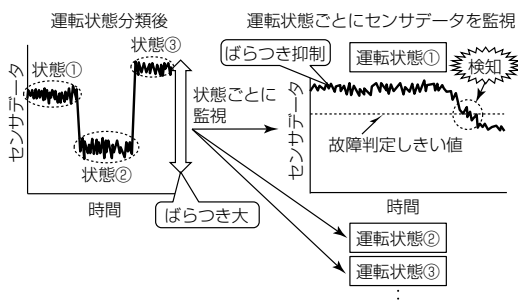


図9. 運転状態分類による検知精度向上

タリングすることによって、類似した運転状態同士でデータを分類することが可能となる。

このように運転状態を分類することで、異常検知に利用するセンサデータのばらつきは低減され、高精度に異常を検知することが可能となる(図9)。

6. データ分析基盤技術

データの大量化、高次元化が進み、人手に依存した分析では、データを有効に活用できないという課題があり、分析作業の自動化が求められている。2章でも述べたとおり、データ分析を進めるうえで、共通化できる部分はできるだけ共通化し、一方で共通化困難な部分についても、カスタマイズの部分を極力削減し、容易に対応できるようにしておく必要がある。この課題に対応するため、個々の分析に応じたデータの加工や分析手順などをシナリオ化し、決められたフォーマットで記述されたテキストを作成し、それを解釈させることで様々な対象に対して分析が可能となるデータ分析基盤技術を開発した。

従来は分析対象ごとに異なるデータの特性や、分析内容に対応するため、個別にアプリケーションを開発していたが、今後は分析機能を共通基盤化し、カスタマイズの部分を極力削減することによる分析の効率化が求められている。

これまでのデータ分析技術開発の取組みによって、データ分析には、次の3種の機能が共通化可能であることを確認した。

(1) 時間窓特徴量の計算

時系列データを比較する部分列の特徴量を計算する機能

(2) 特異時刻選択

統計量のしきい値比較、論理演算によって特異時刻を選択する機能

(3) 実行制御の機能

パラメータを変更しながらシナリオの反復実行や、条件分岐等の制御が可能な機能

そこで、データ分析基盤は、これらの機能を備えた基盤ソフトウェアとして設計し、特徴量計算をユーザー定義関数として追加可能な設計とした。さらに、これらの機能

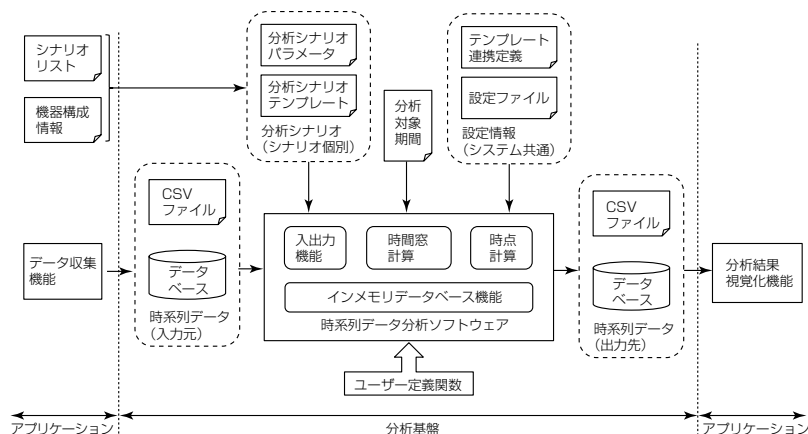


図10. データ分析基盤のアーキテクチャ

は、シナリオで実行可能とした。ここでシナリオとは、使用するデータベース、データ抽出期間、異常判定に使用するアルゴリズムを記述したもので、これらの形式を定義し、またそれを解釈するソフトウェアを開発した。分析者は、シナリオとして入出力を指定した関数を複数並べて記述するだけで、その記述に従った分析結果を得ることができる。これらの結果、汎用的に対応可能な基盤を実現した(図10)。

7. む す び

センサデータを活用した故障予兆検知分析技術等について述べた。しかしセンサデータだけでは故障や品質低下の要因を知ることはできない。要因を分析するためには、設備の使われ方を示す運用情報や、設計情報、保守・点検記録なども必要になる。これらの情報は、現場作業員のノウハウや、文書記録として蓄積された情報であり、今後はこれらの情報とセンサデータを連携させたデータ分析技術の開発に取り組む。

参 考 文 献

- (1) T. Rakthanmanon, et al.: Searching and Mining Trillions of Time Series Subsequences under Dynamic Time Warping, SIGKDD 2012, 262~270 (2012)
- (2) 中村隆顕, ほか: 標本部分列を用いた時系列データ異常検知方式, 電気学会 論文誌C, **136**, No.3, 363~372 (2016)
- (3) 今村 誠, ほか: 時系列データにおけるレグ振動解析, 情報処理学会 論文誌(ジャーナル), **57**, No.4, 1303~1318 (2016)
- (4) 今村 誠, ほか: 設備異常診断用の時系列データ検索言語TPQL, 電気学会論文誌C(電子・情報・システム部門誌), **134**, No.1, 156~167 (2014)

高性能センサデータベース

郡 光則*
米田貴雄*

High-performance Sensor Database

Mitsunori Kori, Takao Yoneta

要 旨

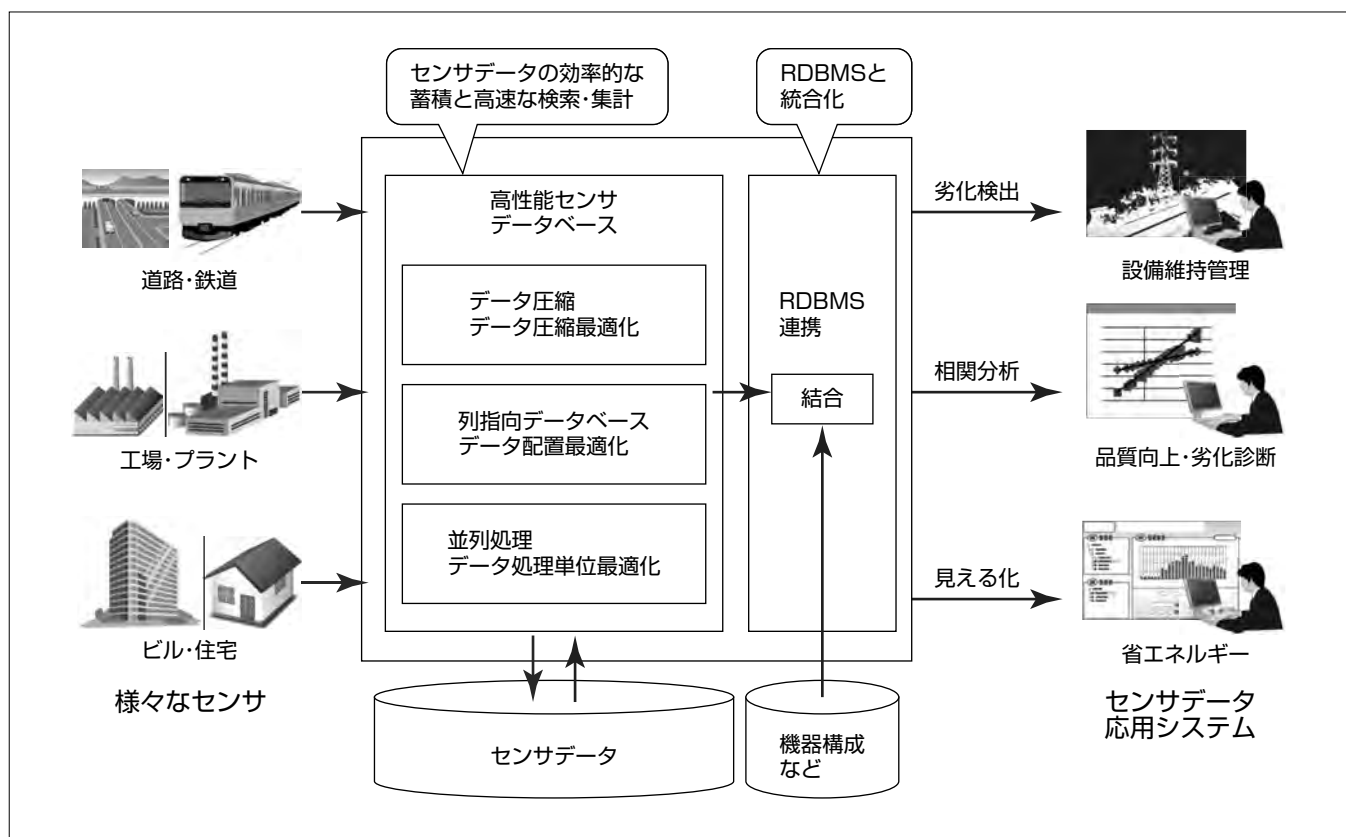
様々な機器がネットワークに接続されるIoT(Internet of Things)の時代を迎え、機器の生み出す大量のセンサデータの活用が進んでいる。道路や鉄道などの社会インフラ設備の維持管理における劣化箇所の検出、工場やプラントの稼働状況の分析による製品品質の向上や劣化診断、ビルや住宅の電力消費量の見える化による省電力など、様々な分野で大量のセンサデータを活用する事例が増えつつある。

しかし、RDBMS(Relational DataBase Management System)に代表される従来のデータベースは大量のセンサデータを効率的に扱うことができなかった。近年では、多数のサーバによる並列分散処理、大容量主メモリを利用したインメモリ処理、フラッシュメモリを利用した高速ストレージの

利用などの対策がとられることがあるが、これらは高価なハードウェアを必要とする。

三菱電機では、これらの課題を解決する“高性能センサデータベース”を開発した。当社が従来研究開発を行ってきた“高速集計検索エンジン”にセンサデータの特徴に応じたデータ圧縮、データ配置、データ処理単位の最適化を適用することによって、RDBMS比で10~1,000倍の高速な蓄積・検索・集計とストレージ容量の1/10~1/1,000の削減を実現した。

また、高性能センサデータベースをRDBMSと統合化し、JDBCなどRDBMSのインタフェースによる検索・集計や機器構成データとの結合などの円滑なデータ連携を実現した。



高性能センサデータベースとその応用分野

高性能センサデータベースは社会インフラの設備維持管理、工場やプラントの稼働状況監視、エネルギー管理などの分野でセンサデータの迅速な活用方法を提供する。センサデータの特徴に合わせた最適化によってRDBMS比10~1,000倍の高速処理を実現し、ストレージ容量を1/10~1/1,000に削減した。RDBMSのインタフェースによる検索・集計やRDBMSで管理するデータとの結合などのデータ連携も可能となる。

1. ま え が き

様々な機器がネットワークに接続されるIoTの時代を迎え、機器の生み出す大量のセンサデータの活用が進んでいる。道路や鉄道などの社会インフラ設備の維持管理における劣化箇所の検出、工場やプラントの稼働状況の分析による製品品質の向上や劣化診断、ビルや住宅の電力消費量の見える化による省電力など、様々な分野で大量のセンサデータを活用する事例が増えている。

増え続けるセンサデータ活用の要求に応えるため、当社ではセンサから得られた大量のデータを高速に蓄積・検索・集計する“高性能センサデータベース”を開発した。

2. センサデータ管理の動向

2.1 センサデータの急増

ネットワークやストレージなどの価格低下を背景に、近年、各種機器の生成するセンサデータの増加が著しい。ある調査によると⁽¹⁾、全世界で生成されるデータの総量は年率約40%で増加しているが、中でも機器の生成するデータの増加が著しく、2013年では全データの2%がセンサデータであったが、2020年には10%を占めると予想されている。

2.2 従来の高速処理技術の課題

センサデータには数値、ビット、IDなどの種類があり、1件当たりのサイズは小さいが膨大な件数が蓄積されることが多い。また、時系列的に連続的に変化する値を取りやすく、しばしば大量一括処理されるといった特徴がある。

ところが、RDBMSに代表される従来のデータベースはこのような特徴を持つセンサデータの管理を主目的として設計されてこなかった。このため大量のセンサデータを扱うシステムでRDBMSを使用するとしばしば処理速度の不足が課題となってきた。

この問題の対策として、1,000台を超える多数のサーバによる並列分散処理⁽²⁾、数十テラバイトに及ぶ大容量主メモリによるインメモリ処理、ビット単価が高いが高速なフラッシュメモリの使用等の方法が知られている。しかし、これらの方法は高価なハードウェアを必要とする。

また、センサデータは一般に機器構成など様々なデータと組み合わせて利用されるため、RDBMSで管理されることの多い各種データとの円滑な連携が必要になる。

3. 高性能センサデータベース

3.1 高性能センサデータベースの特長

2.2節で述べた課題を解決するため、当社では次の特長を備えた“高性能センサデータベース”を開発した(図1)。

(1) センサデータの効率的な蓄積と高速な検索・集計

当社が従来研究開発をしてきた“高速集計検索エンジン”⁽³⁾⁽⁴⁾をセンサデータ向けに最適化し、RDBMS比10～

1,000倍の速度、1/10～1/1,000のストレージ容量を実現した。

(2) RDBMSと統合化

“RDBMS連携”⁽⁵⁾によって、高性能センサデータベースをRDBMSの拡張機能として利用可能とし、RDBMSで管理する機器構成等のデータとの結合を実現した。

3.2 高性能センサデータベースの基本機能

高性能センサデータベースはRDBMSと同様の行・列構造の表(テーブル)の形式でデータを管理する。高性能センサデータベースでは最大100万の列を定義可能とした。これによって、約100万のセンサから同一時刻に計測されたセンサデータを1行に格納することができる(図2)。

高性能センサデータベースでは表1に示す各種のデータ型を扱うことができる。また、高性能センサデータベースの主要機能を表2に示す。

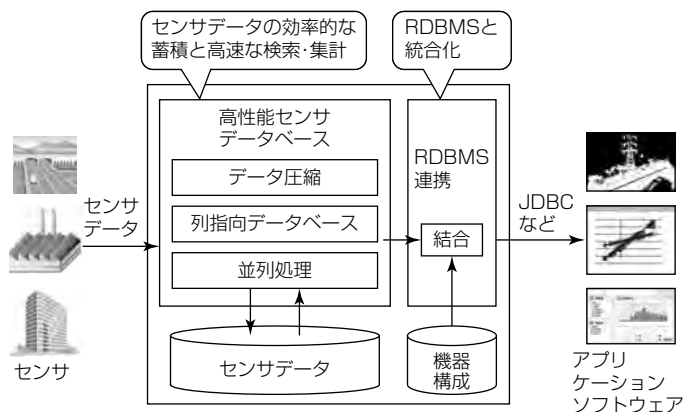


図1. 高性能センサデータベースの構成

最大100万列							
行ID	ロード時刻	計測時刻	センサ#1	センサ#2	センサ#3	...	センサ#N

図2. データ格納形式の一例

表1. 高性能センサデータベースのデータ型

データ型	表記
文字列型	char(n), varchar(n)
整数型	int(n)
実数型(十進数)	dec(p, s)
浮動小数点型	real, double precision
日付型	date
タイムスタンプ型	timestamp

表2. 高性能センサデータベースの主要機能

分類	説明
定義	<ul style="list-style-type: none"> ユーザーの定義、削除、パスワード変更 スキーマ/表/パーティション/ビューの生成/削除/情報取得
ロード	<ul style="list-style-type: none"> 追加ロード、トランケート、トランケートロード
検索	<ul style="list-style-type: none"> 選択条件(where)による行の抽出(選択)、列の抽出(射影) 集合演算(group by)、集合演算結果の抽出(having) 四則演算、ビット演算、論理演算、文字列操作 算術関数(sin/log/exp等)、統計演算(分散、相関係数等) ソート(order by)、取得件数指定(limit/offset) 副問合せ、合併(union)
運用	<ul style="list-style-type: none"> バックアップ、リストア、データ配布

3.3 高性能センサデータベースのシステム構成

高性能センサデータベースはメモリ最小4GBのPCサーバ上で動作し、OSとしてWindows^(注1)又はLinux^(注2)、連携対象のRDBMSとしてPostgreSQL又はOracle^(注3)を使用できる。

高性能センサデータベースは、サーバ1台から利用可能であるが、規模や要求性能に応じてISN(Intelligent Storage Node)と呼ぶサーバを最大256台まで追加できる(図3)。センサデータを長期間保存するシステムでは、運用開始後時間とともに蓄積されるデータ量が増加する。また、小規模の実データで試験運用を行い、効果を確認した後にこの運用へ移行する場合がある。このような場合でもデータの移行やアプリケーションソフトウェアの変更なしにストレージ容量の拡張と処理速度の向上を実現できる。

(注1) Windowsは、Microsoft Corp. の登録商標である。
(注2) Linuxは、Linus Torvalds氏の登録商標である。
(注3) Oracleは、Oracle Corp. の登録商標である。

3.4 センサデータのロード

高性能センサデータベースには基本的にデータを追記する機能は提供しているが、データを1行ずつ更新・削除する機能は提供していない。これは、データを細かい単位で更新・削除する処理は一般に負荷が高く処理速度低下要因になるためである。ただし表を“パーティション”に分割して管理することができる。例えば月単位でパーティションを作成し、1年を経過したパーティションを削除するといった運用を行う(図4)。

3.5 センサデータの検索

高性能センサデータベースはRDBMSを介して検索できる。高性能センサデータベースの問い合わせ文を埋め込んだSQL文によってRDBMSに対して検索要求を行うことで、

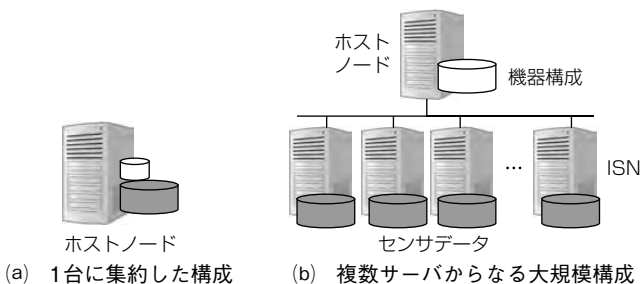


図3. ISNを用いた構成

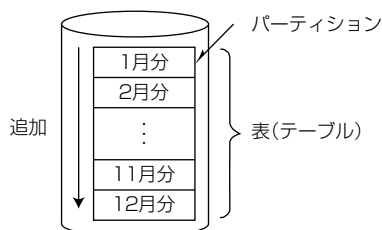


図4. パーティション

高性能センサデータベースの検索を行うことができる。

また、高性能センサデータベースの検索結果とRDBMSのテーブルを結合するなど、データベースの連携が可能である。図5にRDBMSとしてPostgreSQLを使用した場合の連携SQL文の一例を示す。この例では高性能センサデータベースに格納された温度データを日付、部屋番号ごとに集計し、RDBMSに格納されている部屋名称と結合して出力する。

4. 高性能センサデータベースの高速処理技術

大規模データの高速処理の手法として、従来の“高速集計検索エンジン”では次のような方法を用いていた。

- (1) データ圧縮によるストレージ入出力の削減
- (2) ストレージ上への列指向のデータ配置
- (3) プロセッサ内の多数のコアによる並列処理

高性能センサデータベースでは、これらの技術に加え、センサデータ向けの最適化によって高速処理を実現した(図6)。

4.1 データ圧縮

データを圧縮してストレージに格納することによって、ストレージ容量を削減するとともにストレージ入出力の削減による高速化が可能になる⁽⁶⁾。

センサデータには、値が連続的に変化する数値、各ビットが独立に意味を持つビットデータ、離散的な値を取るIDなど様々な種類があり、変化の大きいデータや小さいデータ等様々な性質を持つ。高性能センサデータベースでは、様々なデータに対応するため、700通り以上の基本符号化方式の組み合わせに対して圧縮後のサイズを計算し、サイズの最小となるものを採用する(データ圧縮最適化)。

なお、センサデータの圧縮では、圧縮率向上が可能だが圧縮前のデータを正確に復元できない非可逆圧縮を用いる場合がある。高性能センサデータベースでは圧縮前データを完全に復元できる可逆圧縮を行う。

4.2 列指向データベース

RDBMSでは同一行内のデータをストレージ上の連続領域に固めて配置する行指向データベースと呼ぶ方式が一般的であるが、情報分析用途のデータベースでは同一の列に含まれるデータを固めて配置する列指向データベースと呼ぶ方式を採用する場合がある。

一例として、図2の表でセンサ#1のデータの平均を求

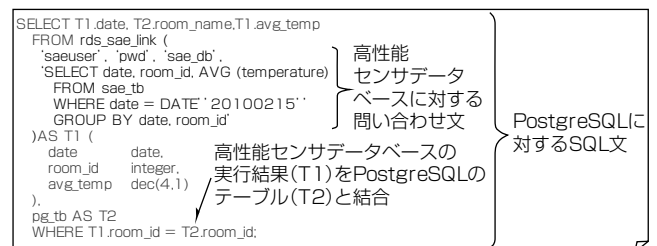


図5. 連携SQL文の例(RDBMSとしてPostgreSQLを使用した場合)

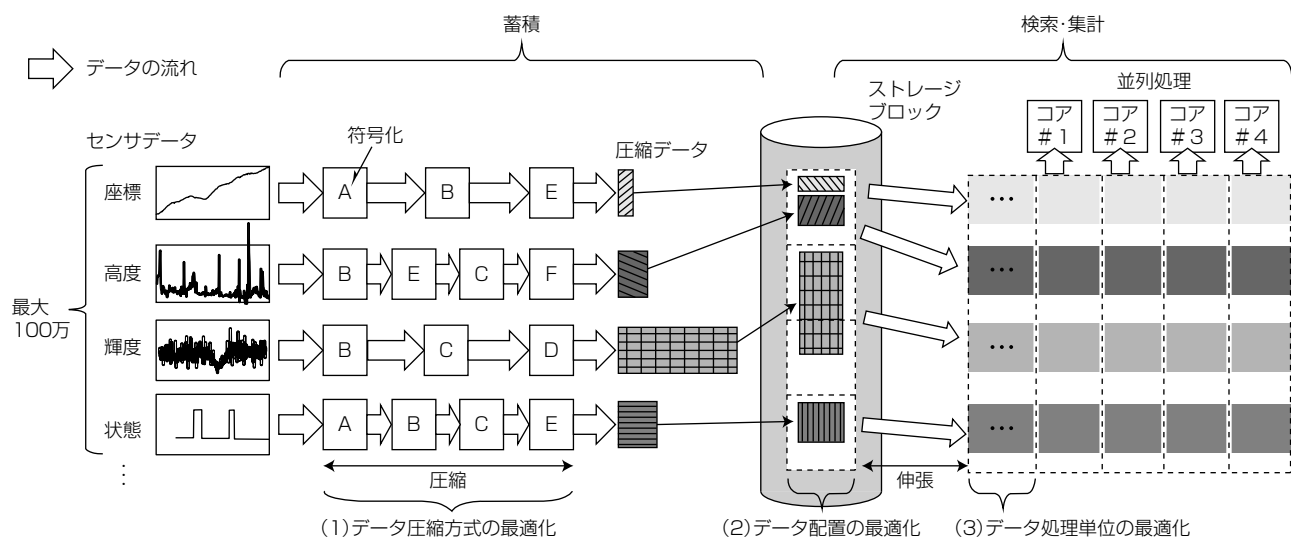


図6. 高性能センサデータベースの高速処理技術

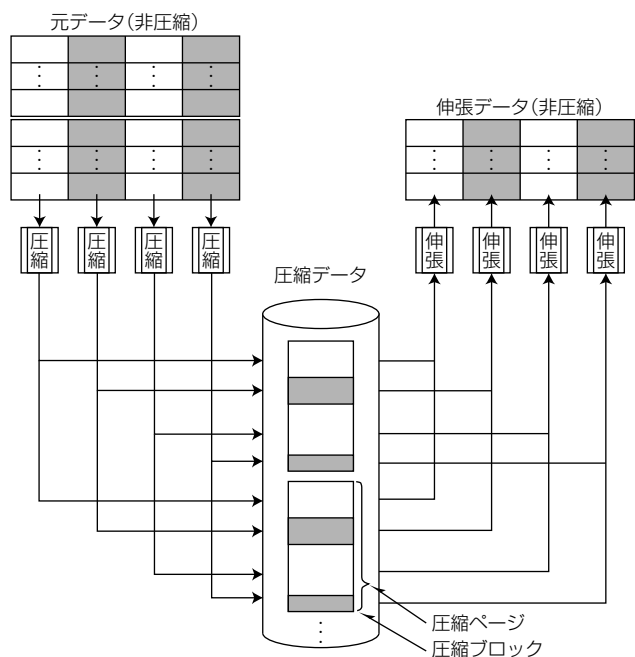


図7. ブロック化トランスポーズド配置

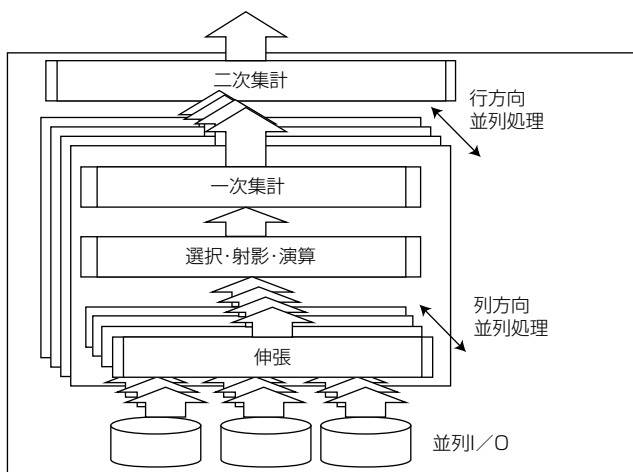


図8. 集計の並列処理の一例

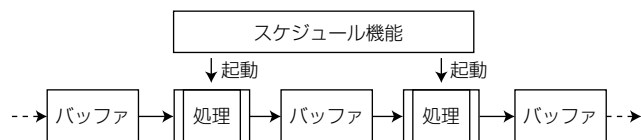


図9. 並列処理の起動制御

める場合、行指向データベースではセンサ#1のデータが分散して配置されるため、全データを読み出した後、センサ#1のデータを抽出する必要がある。列指向データベースではセンサ#1のデータが固めて配置されるため、センサ#1のデータだけを読み出すことが可能である。さらに、センサ#1のデータが連続して配置されるため圧縮率が向上しやすい。

高性能センサデータベースは列指向のデータ配置を基本とし、行指向を複合した配置(ブロック化トランスポーズド配置)を行う(図7)。

ブロック化トランスポーズド配置では、列ごとの圧縮率の差によって、多数の小さい圧縮ブロックと少数の大きな圧縮ブロックが生成されることが多い。ストレージ装置にはストレージブロックと呼ぶ通常512バイト又は4,096バイト固定長の最小アクセス単位があるが、高性能センサ

データベースは、圧縮ブロックが極力ストレージブロックをまたがらないように配置したり、小さい圧縮ブロックを1個のストレージブロック内に配置することによって、ストレージアクセス時間の最小化を図る(データ配置最適化)。

高性能センサデータベースは範囲索引と呼ぶ機能を備えている。圧縮ページごとに列の値の最大・最小値を保持することによって、データ全体を読み出さずに目的とする値が該当する圧縮ページ内に含まれるか否かを高速に判定する。時刻や連番、移動体の座標や積算値など単調に変化することの多い値を検索条件とする検索の高速化に有効である。

4.3 並列処理

近年のプロセッサ性能の向上はコア数の増加に依存する面が大きく、性能向上のためにメモリアクセス効率に注意を払う必要性が高まっている。

高性能センサデータベースでは、データを行又は列方向に分割して並列処理によって高速化を図っている。集計の例を図8に示す。伸張や一次集計、二次集計などの処理はバッファを介してデータを受け渡す(図9)。

各処理の使用するバッファは一般に大きい方が処理の切替えに伴うオーバーヘッドを削減できるが、大きすぎるとデータがプロセッサ内のキャッシュメモリ内に収まらず、処理速度が低下する。高性能センサデータベースでは処理内容に応じてバッファ内の行数を調整することによって速度向上を図っている(データ処理単位最適化)。

表3. 性能評価に用いたサーバの構成

CPU	Intel Xeon ^(注4) E7-4870 2.4GHz Core 10×4
ストレージ	1.2TB, 10,000rpm, 2.5型SAS×4(RAID5)

(注4) Xeonは、Intel Corp.の登録商標である。

表4. 性能評価に用いた処理の内容

処理	電力消費量の集計	
	内容	電力計測値
データ	計測周期	10秒
	センサ数	1,000
	期間	10年分
	データ件数	314億件

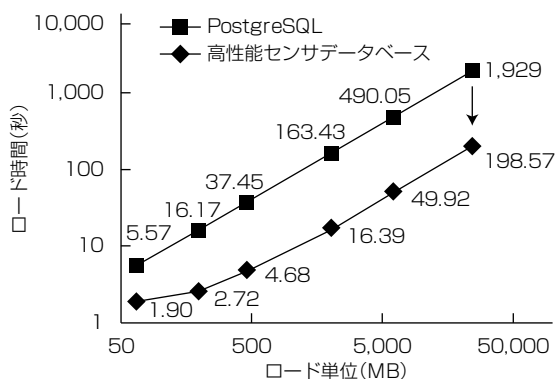


図10. ロード性能の比較

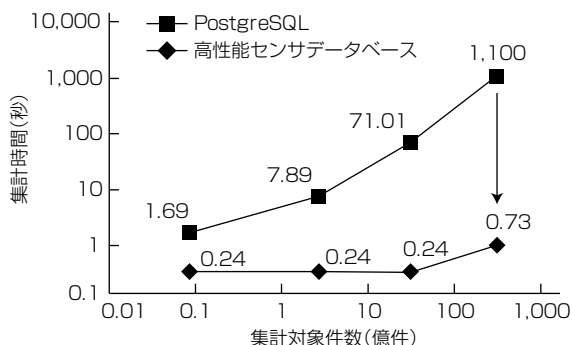


図11. 集計性能の比較

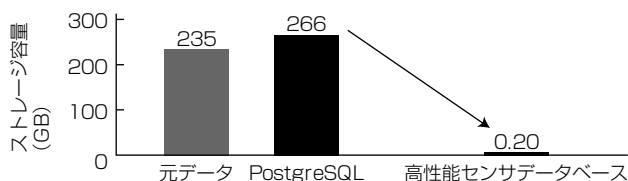


図12. ストレージ容量の比較

5. 性能評価

高性能センサデータベースの性能をPostgreSQLと比較した例を示す。比較に使用したハードウェア構成を表3に、処理の内容を表4に示す。PostgreSQLではロードにpsqlのCOPYコマンドを使用し、検索高速化のため索引を使用した。

ロード性能、集計性能、ストレージ容量の比較をそれぞれ図10、図11、図12に示す。PostgreSQLと比較して10～1,000倍の処理速度向上と1/1,000のストレージ容量削減が実現されている。

6. 高性能センサデータベースの応用分野

高性能センサデータベースは、次の分野を始めとする様々なセンサデータ応用システムへの適用を目指している。

(1) 社会インフラ設備の維持管理

道路や鉄道で周辺構造物の三次元計測データを蓄積し、劣化箇所の検出などを通じて維持管理の効率化を実現。

(2) 工場・プラントの稼働状態管理

電圧、温度、圧力等の計測データを蓄積、製品品質の分析や設備の劣化診断を通じて品質向上や生産効率化を実現。

(3) エネルギー管理

ビルや家庭で計測した電力消費量や温度などのセンサデータを蓄積し、見える化によって省エネルギーに活用。

7. むすび

センサデータの効率的な蓄積と高速な検索・集計を実現し、RDBMSと連携可能な高性能センサデータベースを開発した。今後は様々な応用システムへの適用を進め、そこで得られた知見をフィードバックし、改良を進める予定である。

参考文献

- (1) EMC : The Digital Universe of Opportunities : Rich Data and the Increasing Value of the Internet of Things
<http://www.emc.com/leadership/digital-universe/2014iview/index.htm>
- (2) Apache Hadoop
<http://hadoop.apache.org/>
- (3) 郡 光則, ほか: 高性能並列情報検索技術, 三菱電機技報, **83**, No.12, 705～708 (2009)
- (4) 山岸義徳, ほか: 高速集計検索エンジンとセンサデータベースへの応用, 三菱電機技報, **83**, No.12, 709～712 (2009)
- (5) 竹内文志, ほか: オープンソースDBMS拡張によるセンサデータベースの実現, 情報処理学会第74回全国大会講演論文集, 545～547 (2012)
- (6) 郡 光則: データウェアハウス向け高性能データ圧縮方式, 情報処理学会論文誌, **47**, No.SIG13 (2006)

大規模IoTシステムにおける 計算機リソースサイジング技術

魚住光成* 鶴 薫*
小杉 優*
佐藤尚也*

Computer Resource Sizing Technology in Large - Scale IoT Systems

Mitsunari Uozumi, Yu Kosugi, Naoya Sato, Kaoru Tsuru

要 旨

近年の計算機とネットワークの技術の発展と普及によって、様々なモノの間で情報交換や制御を行うことが可能になってきた。IoT(Internet of Things)システムはセンシングしたデータに対して何らかの処置を施して記憶し、照会に対して記憶からデータを引き出して応えるようなデータ処理を行う。

計算機とネットワークの選択の幅が広がったことで、IoTシステムは様々なハードウェア構成を取り得る。しかし、目的の処理を実現するシステム構成の構成要素の処理能力、数量の確定が、システムの構築で課題となる。

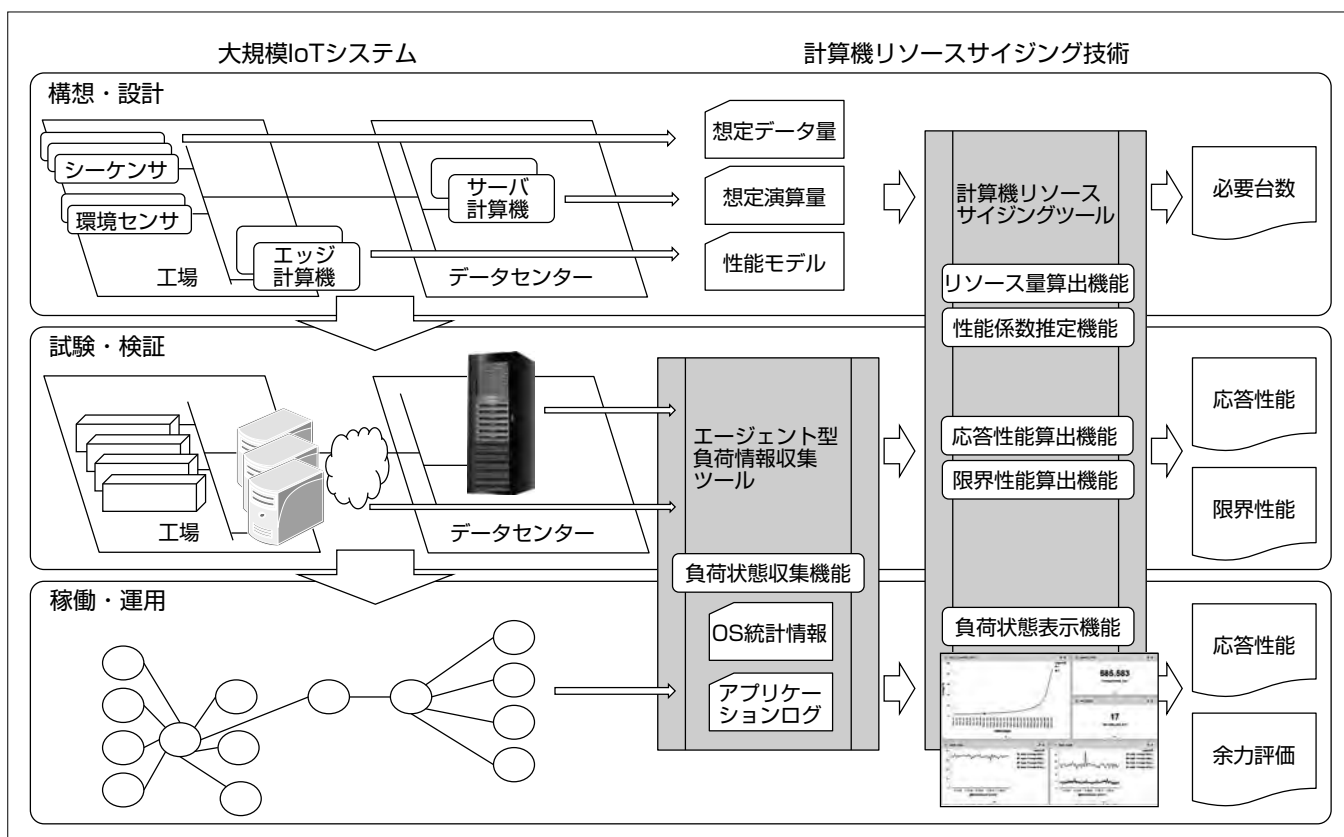
三菱電機の計算機リソースサイジング技術は、システムの構想段階から検証、運用開始後まで、計算機リソースの使用状況を予測、計測、評価し、システムの安定した構築

と稼働を可能とする。

IoTを可能とした計算機とネットワークの技術の発展は、システムの複雑化ももたらしており、直感的なサイジングは不可能である。

当社の計算機リソースサイジング技術では、システムの構成要素を還元的に分解し、それぞれのトラフィックと処理能力を評価することで、ボトルネックとなる要素を抽出するとともに、パッケージソフトウェアなどブラックボックス化された構成要素は、その性能特性をモデル化することで、システム全体の性能の予測、評価を行う。

この技術によって、形態が多様化した大規模IoTシステムの計算機リソースのサイジングを可能としている。



大規模IoTシステムと計算機リソースサイジング

大規模IoTシステムでは、数多くのデータ発生源を対象とするため、計算機リソースのサイジングは開発ステップごとに繰り返すことが重要である。当社の計算機リソースサイジング技術は構想段階から運用監視後までの開発ステップに対応したツールを用意し、システムの開発者、運用者が計算機リソースの必要台数の算出から稼働後の処理能力の余力の評価まで行うことを可能としている。

1. ま え が き

近年の計算機とネットワークの技術の発展と普及によって、様々なモノの間で情報交換や制御を行うことが可能となってきた。

計算機は事業者が設備を抱えるオンプレミスといわれる形態から、計算機リソースをサービスとして提供するクラウドサービスの利用、エンドユーザーに近いところで演算を行うエッジコンピューティングを可能とする安価な計算機リソースまで、選択の幅は広がった。ネットワークは、インターネットや専用線によるプライベートネットワーク、論理的にプライベートなネットワークを実現する各種VPN(Virtual Private Network)などが、有線、無線のネットワーク技術に支えられて実現している。

これらを背景に、個々のモノが相互にネットワークを介して結び付くIoTが現実のものとなってきた。

2. 大規模システムのサイジング

大規模システムの計算機リソースのサイジングは古くから行われている⁽¹⁾⁽²⁾⁽³⁾⁽⁴⁾⁽⁵⁾⁽⁶⁾。

1980年代、大規模な情報処理システムは計算機センターなどに設置された計算機を利用して構築された。当時の情報処理システムは、リソースの割り付けや実行モジュールなどを定義した処理単位をジョブとして記述し、計算機のキューに投入するバッチジョブ型、多数の端末からネットワークを通じて計算機をアクセスするオンライン型が主流であった。

ここで行われたサイジングと大規模IoTシステムを対象としたサイジングの基本的な考え方は変わらない。

2.1 バッチジョブ型

利用者はJCL(Job Control Language)などで記述したジョブを入力装置から投入する。JCLにはアプリケーションプログラムのロードモジュールからアプリケーションプログラムが入力するファイル、出力ファイルや出力装置などが記述されており、ジョブとして一連の処理が完了するまで、利用者が介入することはない。投入されたジョブはジョブキューに蓄えられ、計算機は1件ずつジョブを取り出し演算装置でロードモジュールを実行する。

利用者から見ると、ジョブを投入してから結果を出力装置から取り出すまでに数時間を要する場合もある。一方、演算装置はジョブキューにジョブがたまっている間はその演算能力の100%が使用される。厳密にはディスクアクセスなどCPUと比較して遅いデバイスへのアクセスも伴うため、CPUがアイドルな時間も発生する。これを回避する範囲で複数のジョブを多重に実行することもあるが、今度はディスクアクセスの性能に拘束される。

したがって、ジョブの平均実行時間が T_s のとき、ジョブの投入が $1/T_s$ (件/秒)以上行われるとジョブキューは

無限大に長くなる。投入したジョブが完了するまでの時間に運用上の上限の設定がないならば、 $1/T_s$ がバッチジョブ型の限界性能である。これを超えるためにはより速い演算装置を用意する必要がある。

2.2 オンライン型

利用者が端末を操作すると、計算機の端末制御装置は入力されたデータを受け取り、演算装置上で動作しているオンラインアプリケーションに渡す。オンラインアプリケーションはデータに対する処理を実行して、その結果を、端末制御装置を介して端末に返す。複数の端末がある場合、端末制御装置は端末から受け取ったデータを逐次オンラインアプリケーションに渡し、オンラインアプリケーションはデータを順番に処理していく。

このデータ処理にかかる平均実行時間を T_s とすると、端末からの $1/T_s$ (件/秒)のデータ到着が限界性能であるが、実際は端末に対する応答性能を確保する必要があるため、実用上の限界性能はこれを下回る。

データがランダムに到着する場合、 $0.5/T_s$ (件/秒)のとき平均応答時間は T_s の2倍となり、この負荷を超えると応答性能は急速に劣化し、 $1/T_s$ のとき無限大となる。

3. IoTシステムのサイジングの課題

IoTを可能とした計算機とネットワークの技術の発展は、システムの複雑化ももたらしており、直感的なサイジングは不可能だけでなく、古典的なサイジングの手法も、そのままでは適用が難しくなっている。

幾つかの課題を解決しないと、IoTシステムの計算機リソースのサイジングはできない。

3.1 用途に応じた様々な形態

IoTシステムは、その用途に応じて様々な形態をとる。形態が異なると構成要素間のトラフィックも変わるため、IoTシステム用のサイジングといった一律の手法は成立しない。

3.2 ブラックボックスの増加

システムを構成する要素の多くが、第三者が開発したパッケージソフトウェアなどであるため、その性能特性が不明であることが多い。

3.3 プログラム構成の複雑化とマルチコア

1台の計算機が複数のCPUコアを持つことは一般的になってきている。これを有効に利用するため、ソフトウェアも複数のCPUの割り付け単位を同時に持つマルチスレッドの実装形態を取ることが多い。

こうしたマルチスレッド、マルチコアの構成では、論理的に処理要求を受け付けるスレッドと、実際に演算を行うCPUコアの2層構造となるため、複数の要求を同時並行に処理した場合の時間性能の予測が難しくなっている。

3.4 計測作業の長時間化

データ発生源が多く、また複数の計算機を使用するため、

試験・検証での計測作業が長時間化している。多くの場合、時間性能の評価は計測の事後に行われるため、システムの設定や計測の誤りがあると、もう一度最初から計測作業を行わなければならない。

4. IoTに対応したサイジング技術

当社の計算機リソースサイジング技術では、システムの構成要素の還元的な分解、ブラックボックス化された構成要素の性能特性のモデル化、マルチスレッドに対応した応答性能算出、結果が即時に確認できる負荷情報収集と可視化を実現することで、大規模IoTシステムにおける計算機リソースサイジングを可能にした。

4.1 システム構成要素の還元的分解

計算機リソースサイジング技術では、システムの構成要素を還元的に分解し、それぞれのトラフィックと処理能力を評価することで、ボトルネックとなる要素の抽出とサイジングを行う方法をとる。

IoTシステムはセンシングしたデータに対して何らかの処置を施して記憶し、任意のタイミングで発生する照会に対して記憶からデータを探索して応えるようなデータ処理を行う。このデータ処理のモデルを図1に示す。システム的设计で、図に示した要素は何台かの計算機に分割されて実現される。

例えば、一極集中型の実現方式では図2のように、センシングと照会を行う計算機、処理と記憶を行うサーバ計算機の構成になる。この場合、サイジングを行うべき計算機はサーバ計算機1台となり、入力のトラフィックと処理の実行時間を計算機リソースサイジングツールで評価すれば、サーバ計算機として必要な処理能力や台数は決定できる。計算機リソースサイジングツールでは、この算出を待ち行列モデルに基づいて行っている。

センシングの近傍にエッジ計算機を置き、処理をサーバ計算機と分担しあうエッジコンピューティング型の構成を

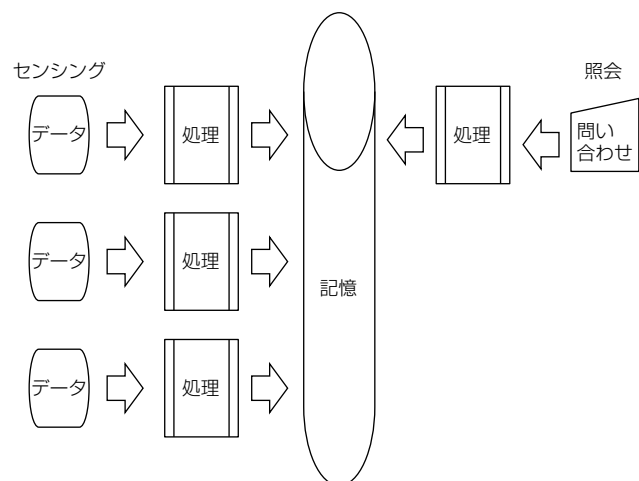


図1. IoTシステムのデータ処理

図3に示す。エッジ計算機がデータの処理をサーバ計算機と分担することで、サーバ計算機の負荷を軽減するとともに、データの集約によるサーバ計算機が受けるデータ数の削減が行える。エッジ計算機とサーバ計算機それぞれの入力のトラフィックと処理の実行時間を計算機リソースサイジングツールで評価すれば、エッジ計算機とサーバ計算機に必要な処理能力や台数は決定できる。

このように、構成要素に還元して計算機リソースサイジングツールでサイジングを行えば、システム全体に必要な計算機の全体の規模を導き出すことができる。

4.2 性能特性のモデル化

計算機リソースサイジング技術では、パッケージソフトウェアなどブラックボックス化された構成要素は、その性能特性をモデル化することで性能評価に組み入れている。

計算機リソースサイジングツールは、計測したデータから対象の性能特性を式の係数として出力する。この式は、以下のような関数としている。

$$T_q = m n (n, \lambda, T_s) \dots\dots\dots (1)$$

ブラックボックスであっても多重度 n 、単体処理時間 T_s を係数として導出することで、任意のトラフィック λ での応答時間 T_q を算出することが可能となっている。

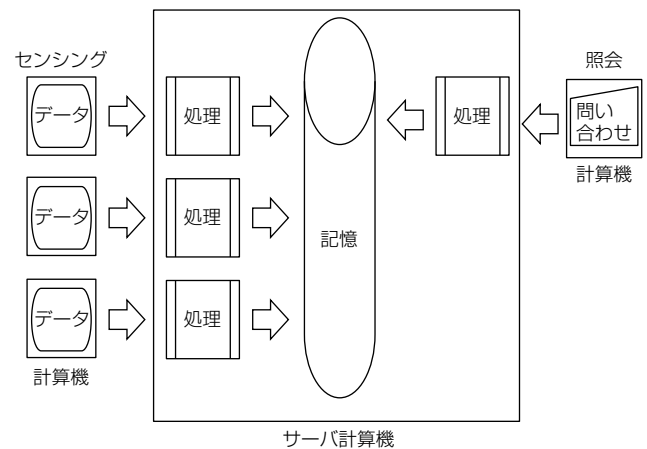


図2. 一極集中型のシステム構成

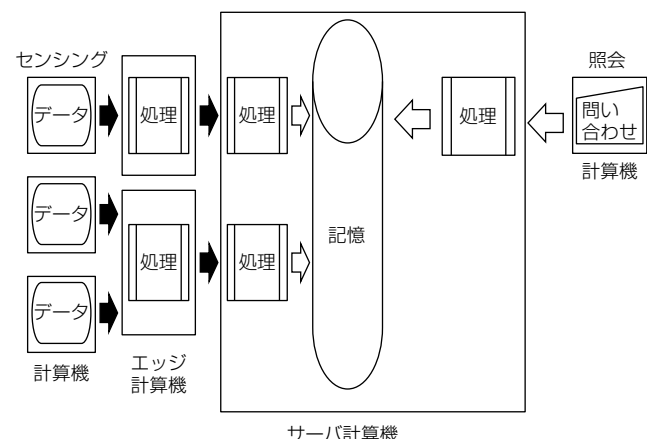


図3. エッジコンピューティング型のシステム構成

4.3 マルチスレッドに対応した応答性能算出

計算機リソースサイジングツールでは、複数のスレッドがマルチコア上で動作する場合の性能を、図4に示すような多段の待ち行列で算出している。

アプリケーションはトラフィック λ を n 個のスレッドで処理しており、それぞれのスレッドはCPU要求を出す。このCPU要求は m 個のコアの内、空いているCPUコアに割り付けられる。この簡略化したモデルによって、任意のトラフィック λ における応答時間 T_q の算出を可能としている。

4.4 負荷情報収集と可視化

計算機リソースサイジングツールは、エージェント型負荷情報収集ツールと連携することで、計測中の性能評価結果の表示を実現している。

図5に性能評価結果表示の画面例を示す。図の左上は、直近の計測値を点で、トラフィックが変わった場合の応答時間の予測値を線で示している。右上の2つの数値は、アプリケーションの管理指標を示している。下段は、計測対象のリソース消費量の時系列な推移を示している。

この機能によって、現在行っている計測が妥当なものか即時に判断できるので、手戻りによる計測作業の効率低下を抑止できる。

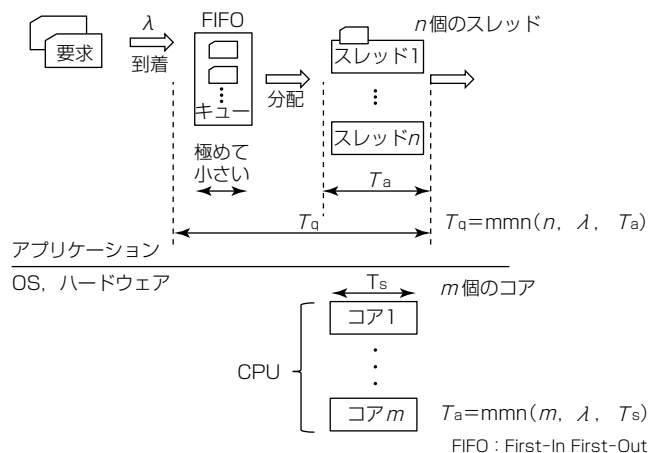


図4. マルチスレッド、マルチコアに対応した性能算出モデル

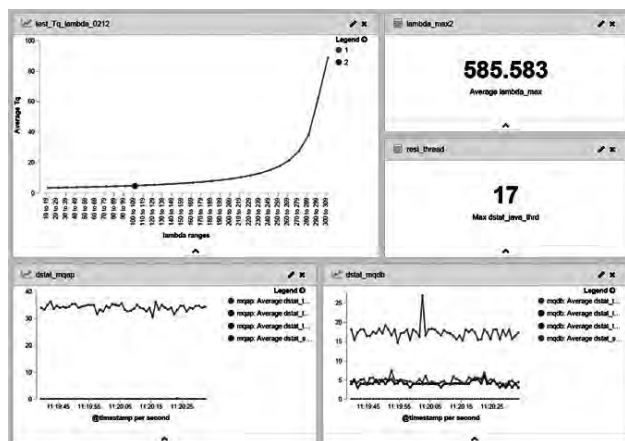


図5. 性能評価結果表示の画面例

5. 考慮すべきリソースの特性

計算機リソースサイジングツールは、指定した条件で必要な計算機リソースの台数や、トラフィックが増加したときの応答時間の予測値を提示する。しかし、個々のサーバ計算機やエッジ計算機的能力によってもその必要台数は変わってくる。計算機の構成要素として、性能に影響が大きいCPU、ストレージ、ネットワークを取り上げ、考慮すべき性能特性を次に挙げる。

ツールの出力結果と合わせてこれらの見極めも行う必要がある。

5.1 CPU

計算機のデータ処理は主にCPUで行われる。演算のみの処理の場合、単体での実行時間はほぼCPUを消費した時間であるCPU時間と一致する。

アプリケーションにプロセスやスレッドなど複数のCPUの割当単位がある場合、これらを順次処理することになるので、CPU時間の平均 T_s とCPU要求の発生密度 λ (件/秒)の $M/M/1$ の待ち行列モデルに沿った性能特性となる。

OSが、CPU要求を蓄積するRUNキューを大きくとれば、要求に対する耐力は増すが、それでも平均 $1/T_s$ を超えることはできない。

マルチコアの場合、CPUの実行を待つRUNキューはそれぞれのコアに存在するが、キュー間の調整も行われるため、複数窓口の待ち行列モデル $M/M/n$ に近似できる(図6)。シングルコアの $M/M/1$ は50%の使用率でCPU時間に対して応答時間が平均2倍に劣化するが、マルチコアの $M/M/n$ では、使用率が上昇しても応答時間の増加の傾向はコア数が多いほど、軽減する。

マルチコアは処理能力をコア数分増加させるだけでなく、高負荷時の性能劣化も軽減する。ただし、仮想化した場合、VM(Virtual Machine)に複数の仮想CPUを割り当て、さらにオーバコミットすると、同時に必要なコア数に関わらず割り付けられた仮想CPU分を物理的なコアを割り付けるため、急速に性能が劣化する。

5.2 ストレージ

ストレージに対するアクセスはシリアルライズされるため、性能特性は待ち行列モデルの $M/M/1$ に従う。したがって、その能力の50%を超えるアクセスがあると急速に性能が

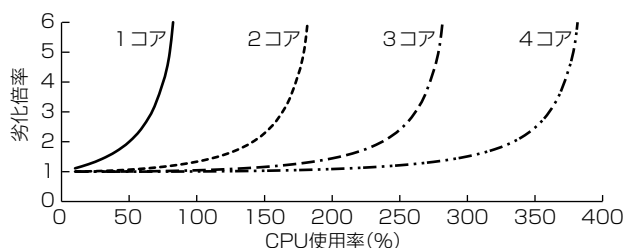


図6. CPU使用率と劣化倍率

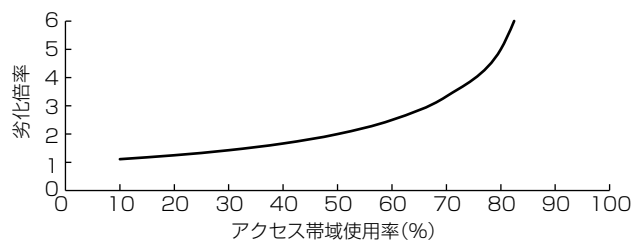


図7. アクセス帯域使用率と劣化倍率

劣化する(図7)。

これを回避するためには、より早いアクセス性能を持つストレージを利用する。SSD(Solid State Disk)やIMDB(InMemory DataBase)などの利用は性能向上に効果がある。ネットワークストレージやVMのストレージは、キャッシュによって性能の遅さを軽減しているが、これは散発的なI/Oに対して効果があるだけで、最大負荷時の能力はやはりデバイスの能力に収束する。

5.3 ネットワーク

ネットワークもストレージと同様、シリアライズされるため性能特性は待ち行列モデルのM/M/1に従う。したがって、より広い帯域を持つネットワークを使用する。

計算機上、ネットワークから到着したパケットは、まずはシングルコアで処理されるため、ここがボトルネックとなることもある。短いパケットが多いときや数Gbpsのネットワークとの接続の場合に課題となる。

6. 開発ステップとサイジングツールの活用

計算機リソースサイジング技術は、システムの構想段階から検証、運用開始後まで、計算機リソースの規模と使用状況を予測、計測、評価し、システムの安定した稼働を可能にする。

それぞれのステップでの活用方法について、次に述べる。

6.1 構想・設計

IoTシステムで扱うデータの規模やトラフィックが議論できる程度の段階から、計算機リソースサイジング技術は活用できる。想定している計算機リソースの規模があるならば、計算機リソースサイジングツールを使って、処理可能なトラフィック量を試算することもできる。

また、実績のないパッケージソフトウェアを使用する場合は、何点かのトラフィックの異なる実機計測を行えば、性能特性は把握でき、性能上のリスクは軽減される。

計算機リソースサイジングツールは、検証環境とは異なるCPUコア数の計算機上での実行性能についても予測することができるため、検証は簡易な設備でも行うことができる。

6.2 試験・検証

計算機リソースサイジングツールとエージェント型負荷情報収集ツールと併用することで、試験・検証を効率的に行うことができる。

アプリケーションに手を加えなくても、OSのリソース

消費の統計情報だけを使って、性能評価を行うことも可能である。

6.3 稼働・運用

稼働、運用の段階でも、計算機リソースサイジングツールとエージェント型負荷情報収集ツールと併用すると、想定内のトラフィックで稼働しているのか、トラフィックの上昇によって、どの程度応答性能が劣化するのか、ライブで確認することができる。

これによって、IoTシステムの性能劣化が発生する前に、計画的に、計算機リソースの増強などの対策を打つことも可能である。

7. む す び

大規模IoTシステムの計算機リソースのサイジングは、原理的には古典的な大規模システムのサイジングと同様に、単体でのリソース消費量から多重時の応答性能の劣化を予測し、許容範囲に入るまでリソースの量や能力を上げていくことを行うことができる。しかし、IoTシステムを可能とした計算機とネットワークの高度化は、システムの複雑化ももたらし、従来手法では対応しにくい課題も生んでいる。

当社の計算機リソースサイジング技術では、システムの構成要素の還元的な分解、ブラックボックス化された構成要素の性能特性のモデル化、マルチスレッド・マルチコアに対応した応答性能算出、結果が即時に確認できる負荷情報収集を実現することで、大規模IoTシステムにおける計算機リソースサイジングを可能にした。

この技術は、システムの構想段階から検証、運用開始後まで、計算機リソースの使用状況を予測、計測、評価し、システムの安定した稼働を可能とするものである。

参 考 文 献

- (1) Molyneaux, I. 著, 田中慎司訳: アート・オブ・アプリケーションパフォーマンステスト, オライリージャパン (2009)
- (2) 市原利浩, ほか: 予備系システムのダウンサイジング手法及び評価, FIT2014(第13回情報科学技術フォーラム), RO-011 (2014)
- (3) Erlang, A.K.: Probability and Telephone Calls, Nyt. Tidsskr. Mat.Ser.B, **20**, 33~39 (1909)
- (4) Kendall, D.G.: Some Problems in the Theory of Queues, J.Roy.Statist.Soc., Ser.B, **13**, No.2, 151~158 (1951)
- (5) Whitt, W.: The Queueing Network Analyzer, THE BELL SYSTEM TECHNICAL JOURNAL, **62**, No.9, 2779~2815 (1983)
- (6) Lavenberg, S.S.: COMPUTER PERFORMANCE MODELING HANDBOOK, Academic Press (1983)