現場データ利活用を実現する情報制御プラットフォーム

遅野井 英樹 Osonoi Hideki
大平 崇博 Ohira Takahiro
武澤 慶 Takezawa Kei
西村 卓真 Nishimura Takuma
横田 大輔 Yokota Daisuke
森 駿介 Mori Shunsuke

近年，現場機器のIoT化が進み，現場機器から入手するビッグデータを利活用することによる新たな付加価値創生やビジネスモデルの実現が期待されている。このため，制御システムにおいて，現場データ収集・利活用，IoTデバイスとの柔軟な接続，これらをオープンに実行する際のセキュリティ確保といった新たな要件への対応が重要になっている。
このような背景の中，日立は共生自律分散コンセプトの下，制御システムにおける現場データを利活用した，新たなソリューション提供に向けた技術開発を進めている。

1. はじめに

止まることが許されない重要な社会インフラを稼働させるため，各インフラの設備を監視制御する制御システムは，信頼性および拡張性が重要である。従来からこれらの制御システムに対し，自律分散コンセプトの下，制御用サーバや制御用コントローラなどの制御ノードが制御に必要となる情報を共有し，個々の制御ノードが共有された情報を基に自律的に動作する情報制御プラットフォームを提供することで，信頼性および拡張性に優れた自律分散制御システムの構築を可能にしてきた[1)]。

一方，近年のセンシング，ネットワーク，ビッグデータ解析の進展により，制御システムでは現場機器のIoT（Internet of Things）化が進んでいる。そこから入手する現場情報を制御システム内で利用するだけでなく，経営層や関連するステークホルダーとも共有・活用し，新たな付加価値創生やビジネスモデルをオープンイノベーションによって実現することが期待されている[2)]。

ここでは，これらの潮流に対応するため自律分散のコンセプトをシステムレベルに拡張した共生自律分散コンセプトにおいて，基盤技術となる情報制御プラットフォームの技術開発について述べる。

2. 制御システムの課題と取り組み

制御システムは，制御用OS（Operating System）が動く制御用サーバ，制御用ネットワーク，制御用コントローラ，また，それらを束ねる制御用ミドルウェアなどから成る情報制御プラットフォームを用いて構築されている。

前述の共生自律分散コンセプトを実現するうえで，制御システムには現場データ収集・利活用，IoTデバイスとの柔軟な接続，これらをオープンに実行する際のセキュリティ確保といった新たな要件が発生する。

こうした要件を満たすため，情報制御プラットフォームに対し，「現場データを収集して解析に適したデータとして提供」，「現場環境に設置されるIoTデバイスとの容易な連携と影響の最小化」，「制御システム向けセキュリティ」という新たな機能の開発を進めている（図1参照）。

これらの技術開発のうち，以下の3点を報告する。

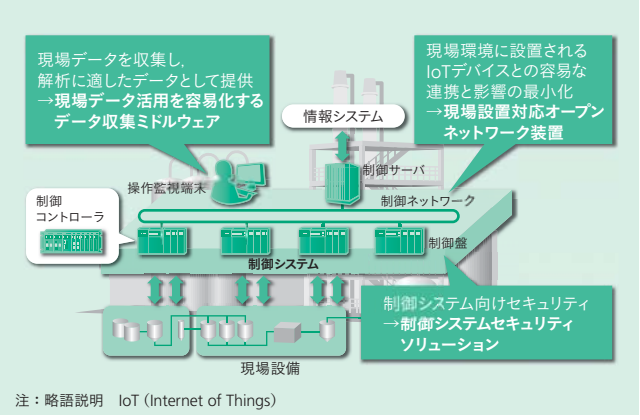


図1｜情報制御プラットフォームが提供する新たな機能
共生自律分散コンセプトを実現するうえで，情報制御プラットフォームに対して，新たな要件を満たすための新機能開発を進めている。

(1) 現場データ活用を容易化するデータ収集ミドルウェア
(2) 現場設置対応オープンネットワーク装置
(3) 制御システムセキュリティソリューション

3. 現場データ活用を容易化するデータ収集ミドルウェア

現場には，エネルギーや経済性の点でさらなる効率化に活用できるデータがあると考えられる。一方，ビッグデータ解析の技術進展により，この現場データを活用したサービスを提供できる環境が整いつつある。そのため，現場データを活用するサービスには，多様な現場データの収集手段が必要であり，この収集には利活用したいデータを容易に取り出せる拡張性が求められる。

3.1 プル型情報収集ミドルウェア

一般的な制御システムでは，制御コントローラが制御対象の状態をセンサーで取得し，アクチュエータを用いて制御する。その状態は監視用データとして処理されて制御ネットワークに送信され，それを制御サーバ（監視装置）が監視している（図2参照）。

ここで送信されるのは，監視装置で監視するためのデータであり，センサーから取得した生の値ではない。例えば，パイプの流量を監視する場合は，流量は温度や圧力といった複数のセンサーの値から計算している。そのため，例えば，個々のセンサーの故障の確認や予兆といった新しいO&M（Operation and Maintenance）サービスをする場合には，制御コントローラが送信しているデータではなく，制御コントローラが内部に持つセンサーの値を取得する必要がある。

しかし，現在の制御システムでこれらの値を取得するには，取得対象データを追加・変更するごとに，制御コントローラ内のソフトウェアや設定を変更しなければならない。これでは制御コントローラの停止など，生産への影響が大きく問題である。

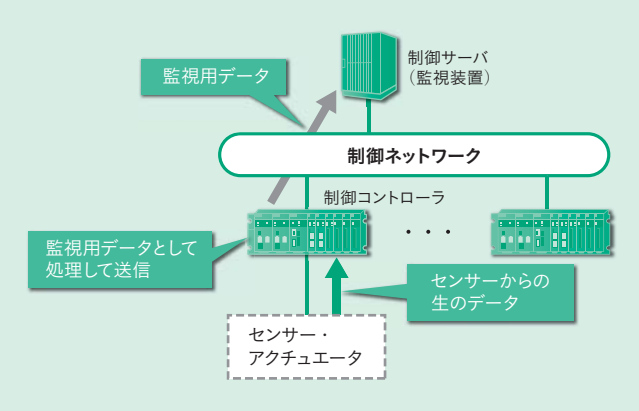


図2｜制御システムでのデータ取得の流れ
制御サーバでは，センサーからの生のデータではなく，制御コントローラで処理された監視用データを取得する。

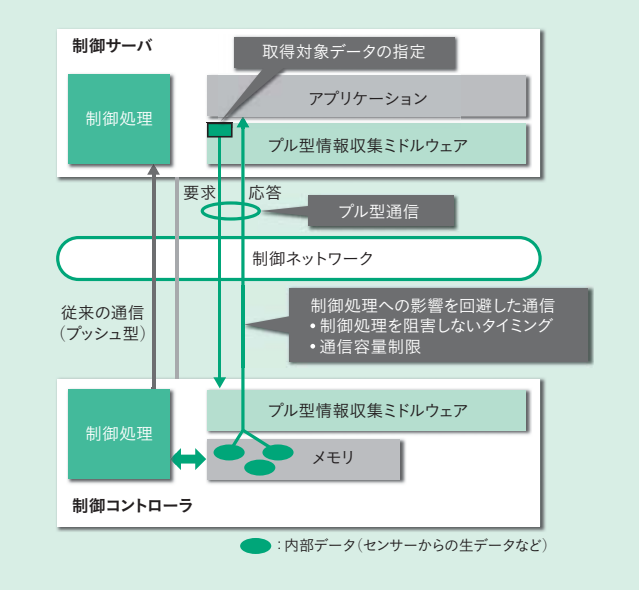


図3｜プル型情報収集ミドルウェアのアクセス機能の概要
制御サーバからのデータ取得要求に対し，制御処理への影響を回避しながら，制御コントローラの内部データを制御サーバへ応答する。

そこで，この問題を解決し，利活用したい制御コントローラ内のデータを，必要なときに取得可能とするプル型情報収集ミドルウェアを開発した。

このミドルウェアは，制御サーバ上で動作するアプリケーションが，制御コントローラ内の取得対象データを指定することで，制御コントローラ内のソフトウェアや設定を変更せずに取得対象データの追加・変更を可能とする。また，制御コントローラからのデータ取得は要求応答型（プル型）で実施し，データ取得の要求を受信した制御コントローラは，制御処理を阻害しないタイミングで，要求されたデータを制御サーバに応答する。さらに，このデータ取得要求によって制御コントローラに過負荷がかかり，制御処理に影響を与えることがないよう，あらかじめ設定した通信容量以下で通信する機能を持っている（図3参照）。

今後は，収集したデータを解析に適したデータに変換する機能の拡張を行っていく予定である。

3.2 稼働監視ミドルウェア

社会インフラシステムが多様化・複雑化するに伴い，システム障害が発生した場合の障害箇所切り分けに要する時間は増加しており，この作業によるロスコスト（損失）は収益の圧迫要因となっている。

制御機器を構成するハードウェア，ソフトウェアは，現状でもおのおのの稼働情報データを取得する手段を持つが，次の問題があり，データの活用が限定的であった。

(a) 原因調査に必要な情報が収集不可

情報を収集するために必要となる保守員の操作が遅れると必要な情報が収集できない。

(b) ログ解析が属人化

情報を解析するためにノウハウが必要であり，特定の人物しか解析できない。

(c) 調査範囲の絞り込みが困難

必要となる情報の特定ができない。

(a)～(c)の問題点に対し，解決手段となる稼働監視ミドルウェアを開発した[3]。この稼働監視ミドルウェアは，以下のコンポーネントによって構成される。

(1) 稼働情報（障害情報）採取ミドルウェア

あらかじめ設定したトリガ（エラーメッセージなど）発生時に，対応する障害情報を自動で採取し，ディスクに保存する。また，すべての種類の障害情報を一括で採取するコマンドを保守員に提供する。

(2) 稼働情報蓄積ミドルウェア

システムに接続されたおのおのの機器の，稼働情報採取ミドルウェアが採取した情報・メモリダンプ情報・ネットワーク情報を，1台の計算機に収集・蓄積する。

(3) アラーム管理ミドルウェア

稼働情報蓄積ミドルウェアが収集した各障害情報に一次解析を行い，推定障害箇所を現地コンソールに出力する。

(4) 障害情報解析ツール

稼働情報蓄積ミドルウェアが収集した情報を基に，より詳細な障害解析を実施する。複数の計算機や障害情報を組み合わせ，時系列や階層化によってGUI（Graphical User Interface）表示するとともに，属人化していた解析ノウハウを学習する機能を有する。

稼働監視ミドルウェアの各コンポーネント［(1)，(2)，(3)］は，おのおのアプリケーション用障害情報の収集および解析コマンドを追加登録可能としており，システムごとに容易にカスタマイズできる。

稼働監視ソフトウェアの現状の目的はロスコストの削減であるが，今後は，増加する海外案件で必要性が高まる遠隔保守サービスに応用していく予定である。

4. 現場設置対応オープンネットワーク装置

高い信頼性と可用性が要求される社会インフラシステムでは，現場に密着した多様なサービスの提供や，精緻かつ新鮮な現場情報の活用など，現場を重視した新たなニーズが生まれてきている。これらのニーズを満たすには，現場の機器間をつなぎ，価値ある現場情報を伝えるための現場ネットワークの構築が不可欠である。

現場ネットワークには，環境条件が厳しく実装スペースに余裕のない現場で，長期にわたって安定稼働できる基盤コンポーネントが必須である。現場ネットワークを構築する基盤コンポーネントには，イーサネット※）技術への対応が要求される。この技術はオープンで汎用性が高くQoS（Quality of Service）や仮想化などの標準化が進んでおり，近年，産業分野にも急速に普及してきている。

4.1 産業用インテリジェントL2スイッチHighR-Switch

これらの要求を満足する現場ネットワーク構築基盤として，長寿命（10年寿命設計）かつ高機能で信頼性と耐環境性に優れる小型10ポートの産業用インテリジェントL2スイッチ「HighR-Switch 300」（伝送速度：100 Mビット/s），「HighR-Switch 3000」（伝送速度：1,000 Mビット/s）を開発した（**図4**参照）。

HighR-Switch 300，HighR-Switch 3000は，SNMP（Simple Network Management Protocol）やSTP（Spanning Tree Protocol），VLAN（Virtual Local Area Network）などの40種類を超える一般的なネットワーク機能をサポートする。

これに加え，プラント制御用ネットワークμΣNETWORK-1000［IEC PAS（Publicly Available Specifications）62953］の基本技術をベースとした独自の光リングプロトコルを搭載している。最大64台構成において，500 ms以内でネットワーク障害からの自動復旧が可能であり，固定障害のみならず間欠障害に対する経路切り替えや，ブロッキング箇所の二重化などの高信頼機能を有する。

また，独自に最適化を図った金属筐（きょう）体構造および部品実装設計により，以下の3つを実現した。

(1) 周囲温度−10℃～60℃への対応

(2) ファンレス，通気孔レス構造による耐塵（じん）性の強化

(3) 耐振強度4 Gの確保

これらの特長を備えることにより，環境条件の厳しい現場設備への設置を可能にした（**表1**参照）。

今後は，大規模システムにも対応可能なイーサネットポートの多ポート化を進めていく予定である。

※）イーサネットは,富士ゼロックス株式会社の登録商標である。

図4｜HighR-Switch
耐環境性の強化により現場設備への設置を可能にした。また，一般的なネットワーク機能に加え，独自の高信頼機能も有している。

表1｜HighR-Switch仕様

HighR-Switch 300/3000の基本仕様を示す。

周囲温度	動作時	−10～60℃
ファン，通気口	ファンレス，通気孔レス	
耐　振	4 G	
適合規格	振動 衝撃 気圧 EMI規格 EMS規格 EMC規格 安全性認定 環境	JIS E3014 1種（0.5 G） JIS E3015 1種（10 G） TB/T 1433-1999，KX3 VCCI class A IEC61000-6-2 IEC61000-6-4 CEマーキング CBテストレポート（IEC60950-1） EU RoHS指令
ネットワーク管理	SNMP SNMP MIB	SNMPv1，SNMPv2c RFC1213 MIB II RFC1215 Traps
光リングプロトコル（IEC PAS62953ベース）	最大伝送距離 最大接続台数 経路切り替え時間	光ループ 総長500 km 64台 500 ms以内
特殊機能	•STP拡張機能（ループガード） •QoS［優先制御，帯域制御（入力ポリシング）］ •ポートセキュリティ（MACアドレスによるアクセス制限） •パケットフィルタ機能（L1～L4レベル） •ループプロテクション •ブロードキャストストーム制御 •ハードウェア障害時のリセットリブート	
自己診断機能	WDT，主メモリECC，キャッシュパリティ，全DC電源電圧監視	
外形寸法	300（W）×180（D）×43.5（H）mm	
設置方向	縦方向，横方向	
電源部	入力電圧範囲	AC 90～250 V
製品寿命	10年	

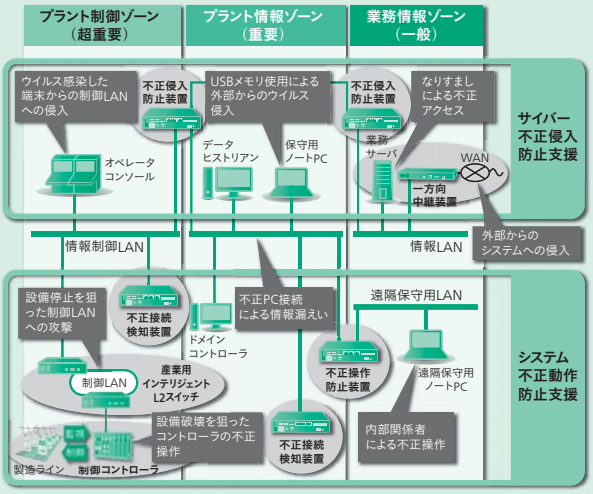
注：略語説明　IEC（International Electrotechnical Commission），PAS（Publicly Available Specifications），EMI（Electromagnetic Interference），EMS（Environmental Management System），EMC（Electromagnetic Compatibility），SNMP（Simple Network Management Protocol），MIB（Management Information Base），STP（Spanning Tree Protocol），QoS（Quality of Service），WDT（Watchdog Timer），ECC（Error Check and Correct），DC（Direct Current），AC（Alternating Current），MAC（Media Access Control），JIS（Japanese Industrial Standards），VCCI（Voluntary Control Council for Information Technology Equipment），CB（Certification Body），EU（European Union），RoHS（Restriction of Hazardous Substances），RFC（Request for Comments）

5.　制御システムセキュリティソリューション

制御システムを狙ったマルウェアであるStuxnetの登場以降，国内外において，サイバー攻撃に対する制御システムの脆（ぜい）弱性が顕在化しており，こういった脅威に対応すべく制御システム向けのセキュリティ対策が必要になっている。

制御システム向けセキュリティ対策では，まず，システムを守るべきセキュリティレベルごとに領域（ゾーン）に分類したうえで，各ゾーンとその接続部である通信路にセキュリティ対策レベルを決め，それぞれに対してセキュリティ施策（予防・検知・拡大防止・回復）を検討・実施することが求められている[4)]。

日立はこの考え方を拡張し，社会インフラ向けのセキュリティコンセプトとして「H-ARCコンセプト」を展開している[5)]。特に制御システムにおけるセキュリティ対策としては，H-ARCコンセプトのうち，あらかじめ定義したもののみ動作させるホワイトリスト（許可リスト）の考え方を利用した強じん性に重点を置いた対策を講じることを推奨し，「サイバー不正侵入防止支援」，「システム不正動作防止支援」の2つを制御システムセキュリティソリューションとして提案している（図5参照）。



注：略語説明　LAN（Local Area Network），USB（Universal Serial Bus），PC（Personal Computer），WAN（Wide Area Network）

図5｜制御システムセキュリティソリューション

幅広い制御システム向けのセキュリティ製品を組み合わせることで，2つの制御システムセキュリティソリューションを提供している。

5.1　サイバー不正侵入防止支援

他のシステムと接続するうえで，サイバー空間経由での不正侵入を防ぐことは，制御システムを外部からの攻撃から守り，その可用性を保つために重要である。また，不正侵入を防止するだけでなく，その導入・運用の負担を軽減することが，制御システムにおけるセキュリティ対策の導入を進めるうえで課題となっている。

そこで，ホワイトリスト型のセキュリティポリシー定義を可能とする不正侵入防止装置では，セキュリティポリシー定義の作成を支援するツールを準備することで，制御システムへのセキュリティ対策の導入を容易にした（図6参照）。

また，一方向中継装置NX Oneway-Bridgeはソフトウェアレス化したデータダイオード装置（ハードウェアレベルでダイオードのように片方向のみ通信を許可する装置）であり，メンテナンスフリー，長寿命化などの特長によって

図6｜不正侵入防止装置

ホワイトリスト型のセキュリティポリシー定義を作成する支援ツールを準備し，制御システムへの導入を容易にした。

図7｜一方向中継装置NX Oneway-Bridge
ソフトウェアレス化することで，運用時の負担を軽減した。装置自体もシンプルな作りとし，間違いを防止している。

運用時の負担を軽減した（図7参照）。

これらの技術により，導入・運用の負担を考慮した不正侵入を防止する対策を拡充させた。

5.2　システム不正動作防止支援

近年増加している標的型攻撃の前では，不正侵入を完全に防止するのは不可能という前提で対策を講じる必要がある。そのため，万が一不正侵入を許した場合に，その被害を最小化するための対策が求められる。情報システムではサイバー攻撃を検知するために，ふるまい検知技術を用いることが多い。しかし，誤検出による影響を許容できないことから，制御システムでの適用は難しく，それに代わって攻撃に対するロバスト性を高める対策を取っている。

不正操作防止装置では，通信データの帯域制限機能や，ネットワーク遮断機能などで，DoS（Denial of Service）攻撃などから重要な設備を防御する。

また，ISA（International Society of Automation）セキュリティ適合性協会（ISCI：ISA Security Compliance Institute）が運営する制御コンポーネントのセキュリティ保証に関する認証制度であるEDSA（Embedded Device Security Assurance）認証取得コントローラであるHISEC 04/R900Eでは，あらかじめ決められたセキュリティ要件に対応することでサイバー攻撃への耐性を高めた[6]（図8参照）。

これらサイバー攻撃に対するロバスト性の高い機器によって制御システムを構成することで，万が一の事態に対しても，制御対象である現場設備への影響を最小化できる。

6.　おわりに

本稿では，共生自律分散コンセプトの下，制御システムの現場データ利活用を図るうえでの最近の課題と技術開発の内容を紹介した。

今後も制御システムは，社会インフラを支える基盤として最新のITの導入が進み，発展していくと予測されるため，引き続き情報制御プラットフォームの技術開発に取り組み，新たなソリューションを提供していく。

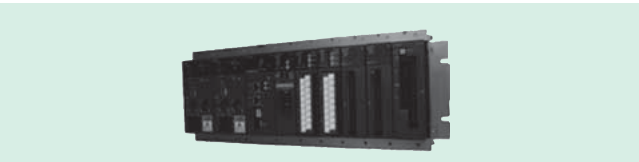


図8｜EDSA（Embedded Device Security Assurance）認証取得コントローラ HISEC 04/R900E
あらかじめ決められたセキュリティ要件を満たすことで，サイバー攻撃への耐性を高めている。

参考文献

1）堀，外：圧延設備での自律分散計算機制御システム，日立評論，72，5，455～460（1990.5）
2）みずほ情報総研株式会社・株式会社みずほ銀行：IoT（Internet of Things）の現状と展望―IoTと人工知能に関する調査を踏まえて―，みずほ産業調査，Vol. 51，No. 3（2015.8）
3）山形，外：社会インフラシステムにおける稼働情報を用いた障害原因調査ツールの提案，情報処理学会第77回全国大会（2015.3）
4）IEC: Industrial Network and System Security, IEC 62443（2013）
5）三村，外：H-ARCコンセプトに基づく日立グループの社会インフラセキュリティ，日立評論，96，3，160～167（2014.3）
6）大久保，外：セキュリティ堅牢性を備えたシステムを構成するプラント監視制御システム，計装，Vol. 58，No. 12，p. 34～37（2015.12）

執筆者紹介

遅野井 英樹
日立製作所 インフラシステム社 大みか事業所
制御プラットフォーム開発本部 制御プラットフォーム設計部 所属
現在，制御システムのコンポーネント開発に従事

大平 崇博
日立製作所 インフラシステム社 大みか事業所
制御プラットフォーム開発本部 制御プラットフォーム設計部 所属
現在，制御システムのミドルウェア開発に従事

武澤 慶
日立製作所 インフラシステム社 大みか事業所
制御プラットフォーム開発本部 制御プラットフォーム設計部 所属
現在，制御システムのコンポーネント開発に従事

西村 卓真
日立製作所 インフラシステム社 大みか事業所
制御プラットフォーム開発本部 制御プラットフォーム設計部 所属
現在，制御システムのコンポーネント開発に従事

横田 大輔
日立製作所 インフラシステム社 大みか事業所
制御プラットフォーム開発本部 制御プラットフォーム設計部 所属
現在，制御システムのミドルウェア開発に従事

森 駿介
日立製作所 研究開発グループ システムイノベーションセンタ
インフラシステム研究部 所属
現在，制御システムの制御データ収集技術の研究開発に従事
博士（情報科学）
情報処理学会会員，計測自動制御学会会員