

# 情報制御プラットフォームのグローバル化とサービス拡張性の強化

清水 勝人  
Shimizu Katsuhito

西島 英児  
Nishijima Eiji

大平 崇博  
Ohira Takahiro

大久保 訓  
Okubo Satoshi

西村 卓真  
Nishimura Takuma

清水 俊樹  
Shimizu Toshiki

新興国を中心に、経済発展の基盤となる社会インフラ整備が都市、エネルギー、鉄道などで進んでいる。先進国では、老朽化した社会インフラのリノベーション要求が高まっている。これらは情報制御システムを中心にした、高信頼で長期運用が必要なシステム構築と情報制御用コンポーネントのグローバルな市場であり、その活性化と伸長が期待されている。

一方、環境負荷が低く、エネルギーや経済性の点で効率のよい社会インフラの実現に向けて、例えば社会インフラ

の持つ現場の情報を基盤にしたビッグデータ利活用などにより、次々に要求される新しいサービス・機能に対応できる多様な拡張性が求められている<sup>1)</sup>。このため、情報制御システムでも、最先端のITの導入と通信のオープン化、および現場のインテリジェント化がより重要になっている。このような背景の中、日立グループは、情報制御プラットフォームのグローバル対応力と、情報制御システムへの最新ITの導入によるサービス拡張性の強化に向けた技術開発を進めている。

## 1. はじめに

日立グループは、一時も止まることを許されない社会インフラの長期安定稼働と高可用性を支える情報制御システム向けの情報制御サーバ、制御用OS (Operating System)、制御用コントローラ、制御用ミドルソフトウェアなどの情報制御用コンポーネント、およびそれらを有機的に組み合わせた情報制御プラットフォームを開発・提供してきた。近年は、特にグローバル市場での調達要件への対応力強化のため、情報制御コンポーネントの国際標準規格への対応に取り組んでいる。

情報制御システムには、高信頼で長期的に持続可能な運用と拡張が必要とされる。特に社会インフラのリノベーションでは、システム維持管理コストの低減と既存ソフトウェア資産の延命が強く求められている。このため、最新の情報システム向けのIT (Information Technology) システムで導入が進んでいるサーバ仮想化技術<sup>2)</sup>について、制御用リアルタイム性を強化し、情報制御サーバに導入するための技術開発を進めている。

一方、従来の情報制御システムはインターネットなどの外部から隔離された環境で運用されることが多かったが、近年は外部のシステムと接続した新しいサービス・機能に

対応できる多様なサービス拡張性が求められている。このような中、情報制御システム向けのサイバー攻撃の脅威に対応した制御システムセキュリティの強化と、現場のインテリジェント化に貢献する耐環境小型コンピュータ開発など、社会インフラの安全・安心とサービス拡張性の向上に寄与するための技術開発を進めている。

## 2. 社会インフラシステムの課題と取り組み

前述のように、情報制御プラットフォームでは、高信頼で長期的に持続可能なシステムの運用と拡張が求められる。また、グローバル市場での調達要件への対応力強化、顧客が創出する新サービスを実現するためのサービス拡張性とセキュリティの強化が重要である(図1参照)。

これらの課題に対応する開発技術のうち、以下4点を報告する。

- (1) 制御用リアルタイム仮想化サーバ
- (2) 制御用コントローラの国際標準認証
- (3) 安全・安心と制御性を両立する制御システムセキュリティ
- (4) 現場のインテリジェント化を推進する耐環境小型コンピュータ

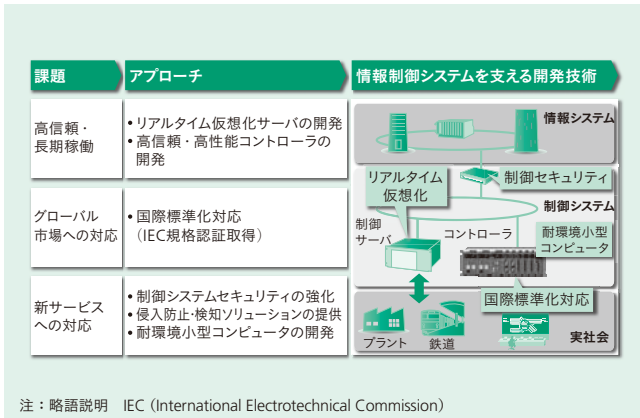


図1 | 情報制御システムを支える開発技術

情報制御システムを取り巻く環境変化とニーズに応じて3つの課題を設定し、情報制御システムの技術開発・製品開発を進めている。

### 3. 制御用リアルタイム仮想化サーバ

#### 3.1 情報制御サーバの動向とサーバ仮想化技術への取り組み

日立の情報制御サーバRS90シリーズは、長期供給・高信頼性を特長とし、発電・鉄鋼など幅広い分野の情報制御システムに適用されている。

近年は情報制御システムでも大規模化が進み、維持管理コストの抑制や、ハードウェアとOSの急速な進化に対応したソフトウェアの延命が課題となっている。また、近年増加している都市開発やエネルギーマネジメントなどの多種多様なシステムが高度に連携するITシステムでは、低コスト化のため、小規模構成で導入した後、段階的に拡張して大規模・恒久的な社会インフラにまで成長可能なことが必要とされる。このため、柔軟性・拡張性に優れた情報制御システムが求められている。

一方、情報システム向けのITシステムでは、維持管理コスト低減のニーズに対応するため、サーバ仮想化技術を利用した仮想化サーバの導入が進んでいる。このサーバ仮想化技術は、計算機ハードウェア上に仮想的なマシンを模擬する仮想マシンを複数動作させることができる技術であ

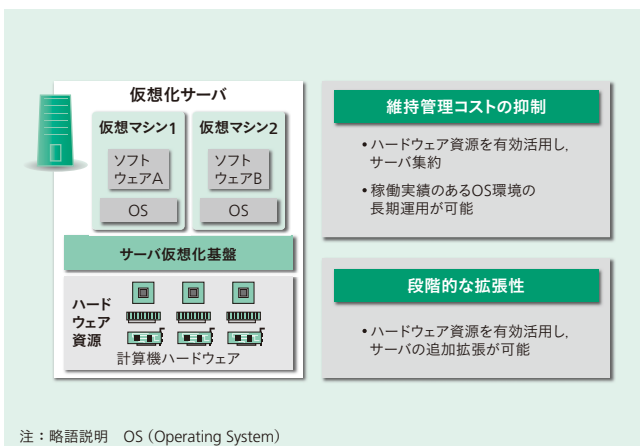


図2 | サーバ仮想化技術

計算機ハードウェア上に複数の仮想マシンを搭載できる技術である。

る(図2参照)。この技術は、仮想マシンに稼働実績のあるOSを搭載することにより、計算機ハードウェアの世代交代時も仮想マシン上では同じOS環境を長期運用することができる。また、負荷率の低いサーバ複数台分を1台の計算機ハードウェアに集約することにより、維持管理コストを低減できる。

そこで、情報制御サーバにサーバ仮想化技術を導入した、仮想化サーバでも情報制御サーバ特有の要求を満たす制御用リアルタイム仮想化基盤ソフトウェア(以下、「RT仮想化基盤」と記す。)の開発により、制御用リアルタイム仮想化サーバを実現した。

情報制御サーバには、現場設備を監視・制御するという役割があるため、10年に及ぶ長期運用、現場設備を制御する処理のリアルタイム性の確保、サーバ障害時に処理の連続性を保ち、現場設備の安定稼働を実現する高可用性、障害原因を確実に取り除く障害解析性、迅速で確実な保守性といった従来の要求がある(図3参照)。ここでは、RT仮想化基盤におけるこれらの要求への具体的な対応について述べる。

#### 3.2 仮想マシン内処理の制御用リアルタイム性確保

情報制御サーバに求められる制御用リアルタイム性として、実行する処理が確定的な順序で動作し、処理結果を予測できる予測可能性、定められた周期で動作を開始する定期性、動作開始要求を受けた処理プロセスが実際に動作を開始するまでの遅延時間を抑える低レイテンシ(遅延時間)などが挙げられる。汎用の情報系システムで使用されているサーバ仮想化技術の場合は、複数の仮想マシンを同時実行する際の処理競合が発生することがある。また、仮想マシン内のソフトウェアから物理ハードウェアへのアクセス処理をサーバ仮想化基盤によってエミュレートして実行するため、仮想マシン内のソフトウェアの処理遅延が発生す

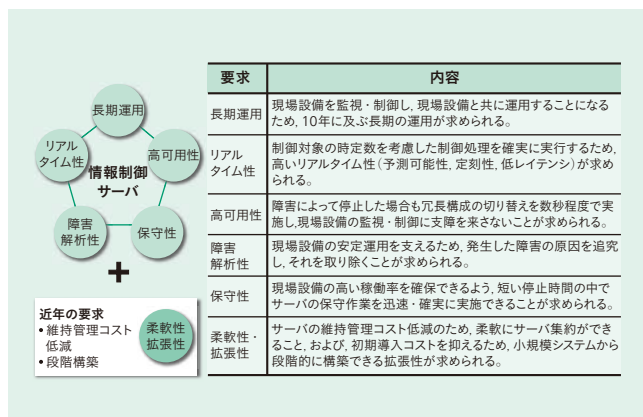


図3 | 情報制御サーバへの要求内容

長期運用や高可用性などの要求に加え、柔軟性・拡張性の向上が求められている。

ることがあり、レイテンシが揺らぐという課題がある。

このため、今回開発したRT仮想化基盤では、仮想マシンが利用するプロセッサ、ディスク、ネットワークといったハードウェア資源を仮想マシンごとに占有可能とする資源分割機構を提供している。この機構により、仮想マシンの同時実行時の処理競合を排除した。また、仮想マシン内のソフトウェア処理を実行するプロセッサのコアと、RT仮想化基盤の処理を実行するプロセッサのコアを分けることにより、仮想マシン内のソフトウェア処理のレイテンシを一定時間に抑えることができる。これにより、サーバ仮想化技術によるレイテンシ揺らぎの課題を解決し、その他の予測可能性や定刻性に対する施策と合わせ、仮想マシン内処理の制御用リアルタイム性を確保した(図4参照)。

### 3.3 仮想マシンの高可用性の実現

これまでの情報制御システムでは、情報制御サーバを冗長構成とし、障害発生時にはソフトウェアを実行する計算機ハードウェアを高速に切り替え、処理の連続性を保つことで可用性を強化してきた。仮想化技術を適用する場合も同様に、仮想化された情報制御サーバを搭載する計算機ハードウェアを冗長構成とし、高速な切り替えを可能にすることで高可用性を実現する。

これまでは、計算機ハードウェアに装備するリセット機構を利用し、障害検知した後に計算機ハードウェアを停止することにより、確実に高速な切り替えを行っていた。RT仮想化基盤でも、このリセット機構を利用して高速な切り替えを可能にした。さらに、RT仮想化基盤では1台

の計算機ハードウェア上で実行される複数の仮想マシンのうち、障害の発生した1台の仮想マシンのみをリセットして待機系の計算機ハードウェアへ切り替えできる機構も提供し、他の仮想マシンについては切り替えをしない切り替えモードも実現した[図5(1)参照]。これにより、障害の発生していない他の仮想マシンの処理への影響を極小化することができる。

また、情報制御サーバの運用面では、ソフトウェアの入れ替えなどでサーバを停止する際は、現場設備の連続運転に支障がないように冗長構成のサーバのうち1台は動作を継続しておき、1台ずつ交替で停止して保守作業を実施することが多い。そのため、RT仮想化基盤では、仮想マシンごとに手で停止できるようにして前述の運用手順を実現した。一方で、仮想マシン単位で切り替えを行った場合、計算機ハードウェア上では実行系の仮想マシンと待機系の仮想マシンが混在し、計算機ハードウェアの部品交換などの保守作業が実施しにくい。このため、RT仮想化基盤では、自動的に当該計算機ハードウェア上のすべての仮想マシンを一括切り替えできるモードも提供し、運用性を高めた。

### 3.4 仮想化サーバでの障害解析性の強化

サーバ仮想化技術では、複数の仮想マシンと仮想化基盤処理が並行して動作するため、処理遅延の発生時などに障害解析が煩雑となる。また、おのおのの仮想マシンや仮想化基盤処理は独立した時刻を持つため、動作トレース情報を収集し、稼働情報を時系列に参照することが困難である。

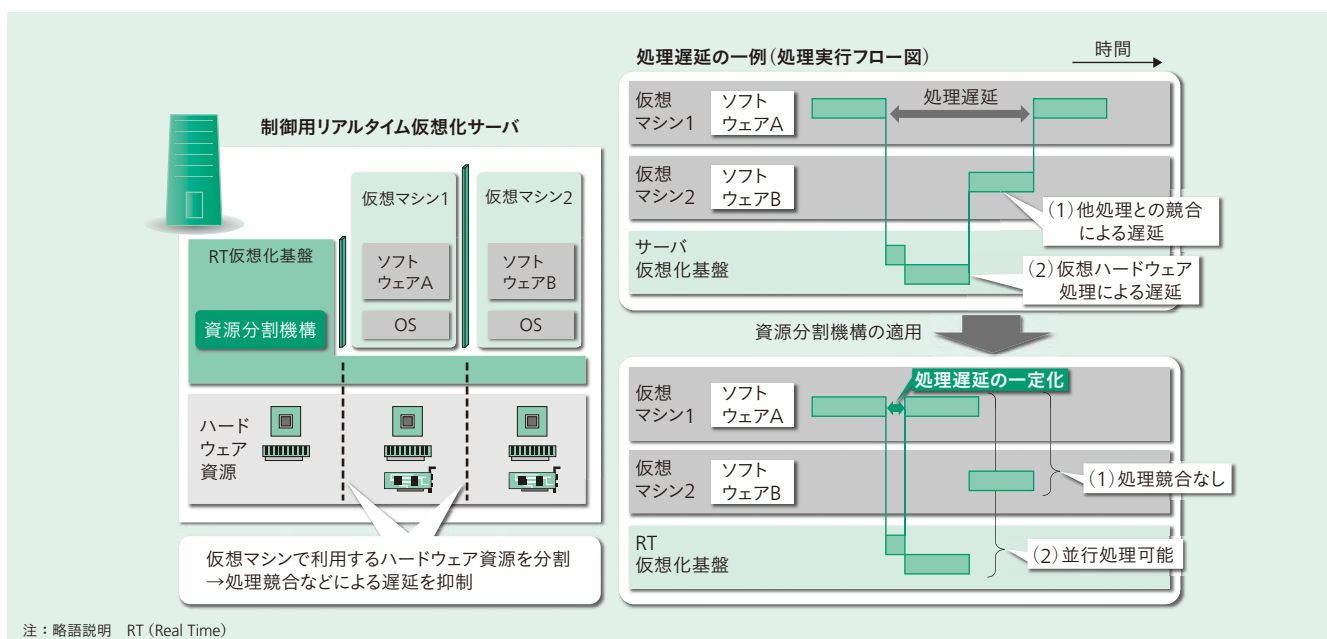


図4 | 制御用リアルタイム性の確保

RT仮想化基盤の資源分割機構の効果例を示す。右上のタイムチャートでは、(1)、(2)によってソフトウェアAの完了が遅れることがあるが、資源分割機構を適用した右下のタイムチャートでは、ソフトウェアAの処理遅延が一定化される。



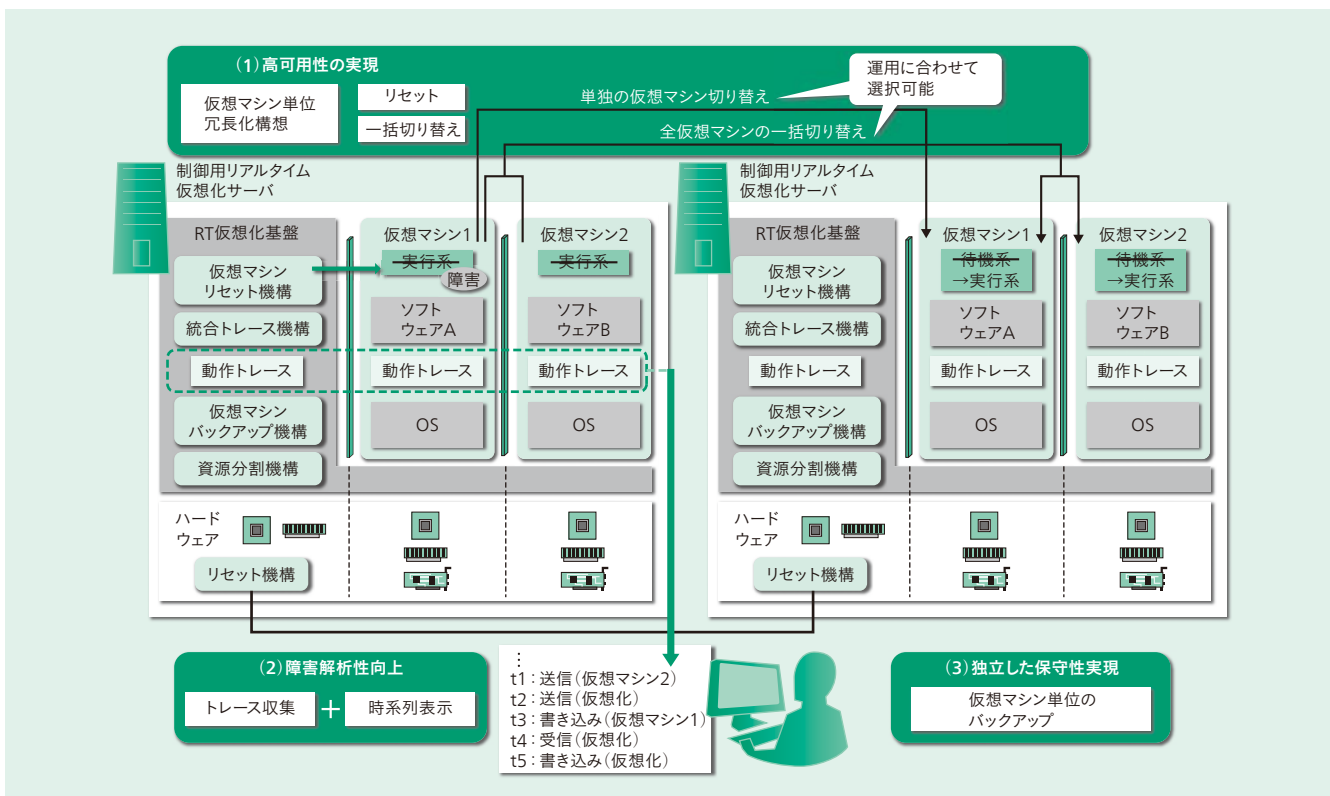


図5 可用性・障害解析性・保守性の強化

リセット機構を利用した高速な切り替え，統合トレース機構を利用した解析性の改善，および資源分割機構により，保守性が向上した。

そのため，RT仮想化基盤では，各種の動作トレース情報を時系列に参照可能とする統合トレース機構を提供した。これにより，仮想マシン内の動作とRT仮想化基盤の処理動作，他の仮想マシン内の動作を，一貫した動作として把握することができ，どの箇所の影響によって処理遅延が発生したかを迅速に特定できるようにした〔図5(2)参照〕。

### 3.5 仮想マシン間で独立した迅速・確実な保守性の実現

情報制御システムでは，制御対象の現場設備ごとや制御機能ごとに情報制御サーバを分割することが多く，比較的小規模なサーバになる傾向がある。このため，ソフトウェアのバックアップ作業を行う場合には，当該の情報制御サーバ全体をシステムバックアップすることが多い。複数の仮想マシンを搭載する場合には，個別の仮想マシンごとにソフトウェアの保守が必要となることが考えられるため，RT仮想化基盤では仮想マシン単位でシステムバックアップを取得できるようにした〔図5(3)参照〕。

一般にバックアップ処理では，ディスクから大きなデータを媒体に格納するため，この処理が稼働中の他の仮想マシンの動作に影響を与えないようにする必要がある。このため，前述の資源分割機構を利用し，バックアップ処理が利用できるプロセッサ時間やディスクアクセス帯域などの資源を制限して動作するモードを提供した。これらにより，仮想マシンごとに独立した迅速・確実な保守作業を可

能にした。

## 4. 制御用コントローラの国際標準認証

制御用コントローラへの安全・安心に対する要求が高まっており，これらに対応した国際標準規格に準拠した製品開発を進めてきた。

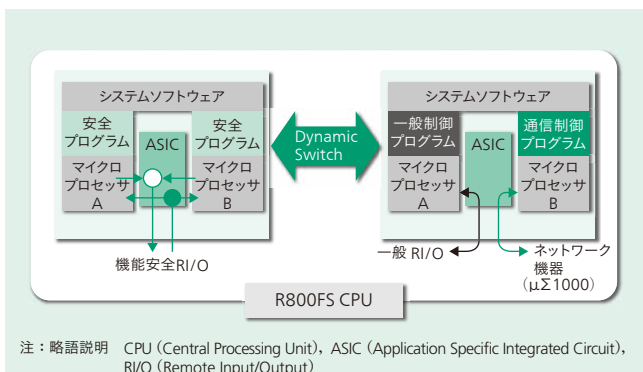
制御用コントローラにおける安全・安心のための国際標準規格には，機能安全，電気安全，EMC (Electromagnetic Compatibility：電磁両立性)，および制御システムセキュリティの認証などがあり，これらの国際標準規格に準拠した製品の開発を進めている。

ここでは，機能安全規格に準拠した制御用コントローラの開発について述べる。

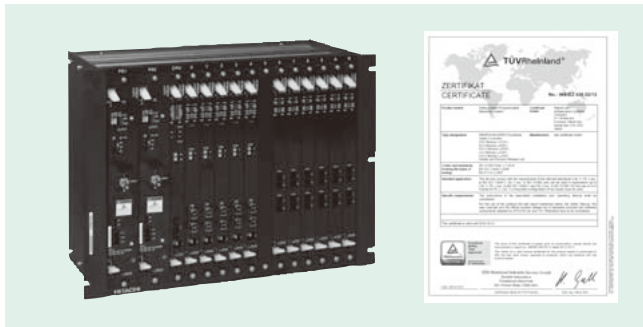
### 4.1 機能安全コントローラR800FS

日立グループは，機能安全規格 (IEC 61508：2010 Edition2.0<sup>3)</sup>) 準拠の機能安全コントローラ HISEC R800FS (以下，「R800FS」と記す。) と機能安全RI/O (Remote Input/Output) を開発し，R800FSバージョン1について，2010年にドイツのTÜV Rheinland Holding AG社より認証を受けた。

機能安全規格では，ハードウェアは故障率および自己診断率が所定の規定値を満たすこと，ソフトウェアは安全を脅かす設計不良を作り込まないことを保証する開発プロセ



**図6 | R800FS CPUにおける機能安全制御と汎用制御の両立**  
2つのマイクロプロセッサにより、診断率を向上し、機能安全制御と汎用制御演算を両立した。



**図7 | 機能安全コントローラR800FS CPUユニット (左) と TÜV Rheinland社による認証状 (右)**  
性能向上を図ったバージョン2として2013年に更新認証を受けた。

スの認証が必要である。また、故障時には、現場設備への制御出力信号が安全側の値となるフェイルセーフ設計が求められる。

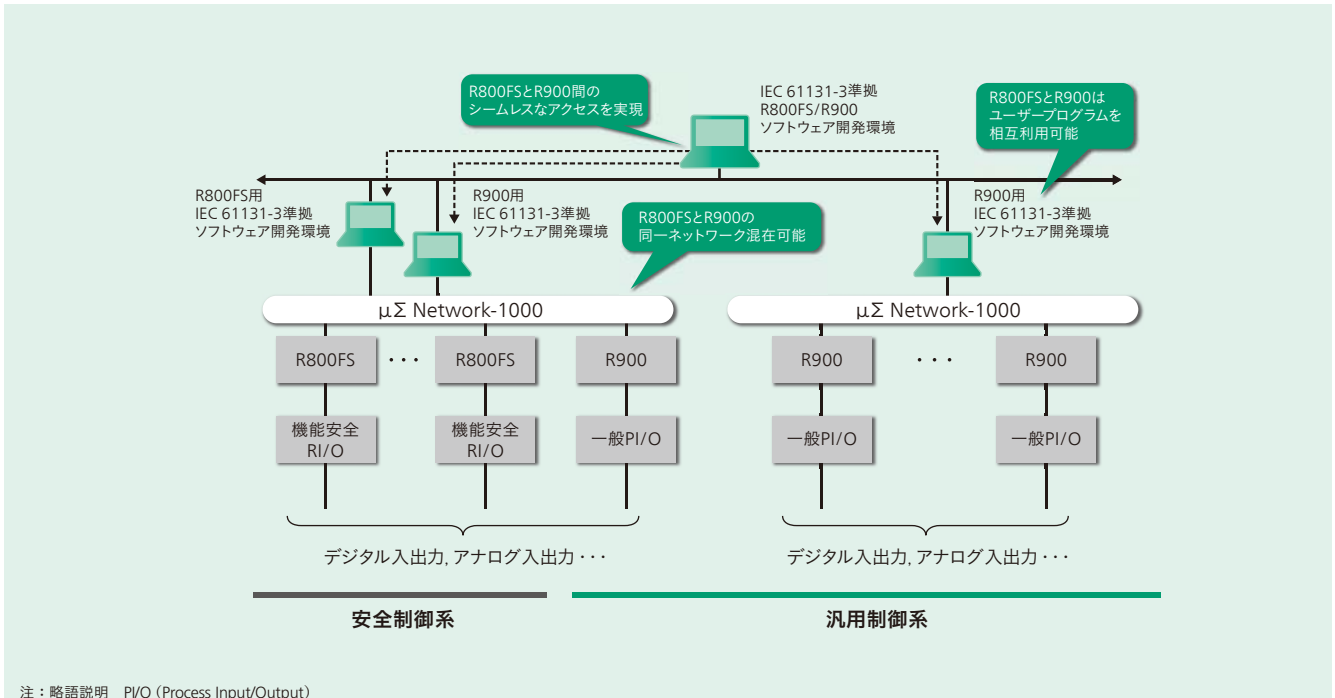
R800FSでは、安全保護系などに要する機能安全プログ

ラムと、汎用制御系や情報処理を行う一般プログラムの両方のユーザーアプリケーションプログラムを搭載しているため、相互に補完しながら柔軟性の高い制御機能を実現することができる。機能安全プログラムは、R800FSのCPU (Central Processing Unit) に搭載した2台のマイクロプロセッサによって並列演算を実施する。その演算の途中値と結果についてASIC (Application Specific Integrated Circuit) 内部の照合機能による診断を行い、安全な演算の実行と制御出力を実現する。一方、一般プログラムでは、マルチプロセッサを生かした柔軟で高速な演算処理ができる。機能安全RI/Oでは、内部回路を二重化したASICによる入出力照合により、高い自己診断率を実現した (図6参照)。

**4.2 可用性・保守性と性能の向上をめざすR800FSバージョン2**

機能安全の思想は、故障発生時には制御出力を停止させることが基本であるため、設備の可用性が低下することがある。これに対し、故障発生時にも、安全に制御継続を可能とするための高可用性と保守性向上をめざした製品として、R800FSバージョン2 (以下、「バージョン2」と記す。)を開発し、2013年にTÜV Rheinland社より更新認証を受けた (図7参照)。

R800FSでは、CPUとRI/O間はリモート通信を行い、その通信路は可用性向上のためのリング構成による完全二重化とした。また、多重故障を未然に防ぐため、バージョン2ではノンインテリジェントな通信モジュールを含む全モジュールから障害情報を取得する機能を実装し、障害発



**図8 | Unified Architectureの構成**  
機能安全を有機的に組み込み、拡張性の高いシステム構築ができる。

生をいち早く検出可能とした。さらに、通信回線の誤接続診断と断線箇所検出機能を備え、高い保守性を得た。

CPUとRI/O間のリモート通信には、安全通信を適用している。一般に安全通信を実現する安全レイヤ処理にはソフトウェアが介在し、通常通信よりも処理が多くなる。バージョン2では、性能向上のため、安全レイヤ処理をハードウェアで実現した。これにより、ソフトウェアとハードウェアの並列処理が可能になり、バージョン2では、R800FSバージョン1対比で50%以上の高性能化を実現している。

さらに、電気安全規格UL 61131-2とCAN/CSA E61131-2の認証を取得し、IEC 61131-2で規定される環境・EMC仕様、およびIEC 61326-3-1で要求される機能安全用EMC仕様にも対応した。

### 4.3 柔軟なシステム構築を可能にするUnified Architecture

機能安全コントローラR800FSは、一般制御用コントローラR900、産業用PC (Personal Computer)、および情報制御サーバなどを同じ制御ネットワークに接続し、相互にデータ交信可能とする。また、IEC 61131-3準拠のプログラミング言語によるソフトウェア開発環境によってプログラミング環境を統合し、ユーザープログラムを相互に搭載して運用することができるようにする。これにより、ユーザビリティが向上するとともに、情報制御システムの中に機能安全を有機的に組み込むことができ、より拡張性が高く安全な情報制御システムを構築・運用できる(図8参照)。

## 5. 安全・安心と制御性を両立する 制御システムセキュリティ

### 5.1 制御システムセキュリティの考え方と全体像

近年、制御システムを狙ったマルウェアであるStuxnetの登場により、国内外において、サイバー攻撃に対する情報制御システムの脆(ぜい)弱性が顕在化してきている。これに対応するべく、欧米では、制御システムセキュリティの国際規格の制定が加速し、国際認証取得の調達要件化が進んでいる。一方、日本でも技術研究組合制御システムセキュリティセンター(CSSC: Control System Security Center)を中心に、制御装置向けのセキュリティ認証であるEDSA(Embedded Device Security Assurance)認証スキームの立ち上げが開始されている。

しかし、情報制御システムは、長期間にわたる設備増設や機能拡張に対しても、稼働し続けることが必須であり、稼働システムごとの運用に最適なシステム構成により、制御用コントローラから情報制御サーバ、情報サーバやデー

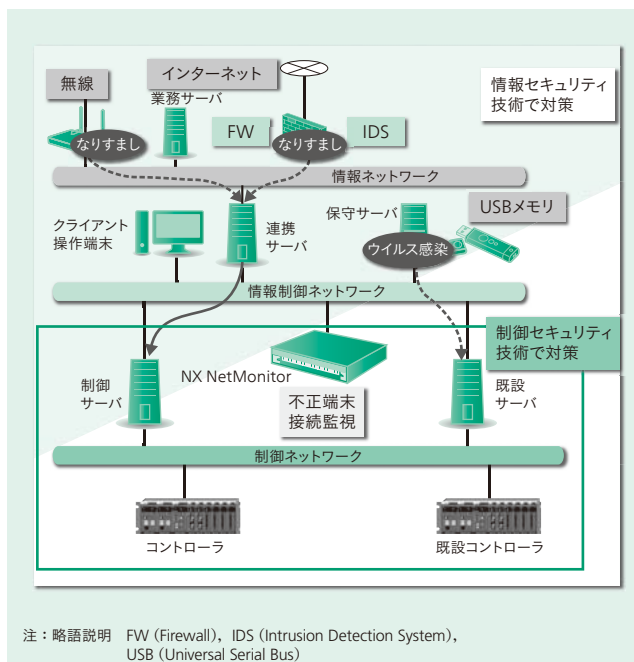


図9 | 制御システムへの適用例

情報セキュリティ技術と制御セキュリティ技術の併用で対応する。

データベースシステムまで多種多様なシステムが混在している。そのため、情報制御システムのサイバーセキュリティを確保・維持するには、FW (Firewall)、IDS (Intrusion Detection System)などの情報セキュリティ製品の採用と国際規格、国際認証取得に対応した制御セキュリティコンポーネントと制御システムの長期運用に対応可能な情報制御ネットワークセキュリティ製品を組み合わせる必要がある(図9参照)。

### 5.2 制御セキュリティコンポーネント

制御コンポーネントのセキュリティを評価する手段として、日立グループはEDSA認証に注目している。EDSA認証は、ISAセキュリティ適合性協会[ISCI: ISA (International Society of Automation) 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り、セキュリティの強さを示す評価レベルごとに、必要な評価項目が定義されている(表1参照)。

CRT (Communication Robustness Test) は、対象装置が

表1 | EDSA認証の評価項目と評価レベル

EDSA (Embedded Device Security Assurance) 認証では、セキュリティの強さを示す評価レベルごとに、必要な評価項目が定義されている。

| 評価項目 | 内容                         | 評価レベル (評価項目数) |         |         |
|------|----------------------------|---------------|---------|---------|
|      |                            | Level 1       | Level 2 | Level 3 |
| CRT  | 通信の堅牢性テスト                  | 69            | 69      | 69      |
| FSA  | セキュリティ機能の実装評価              | 21            | 50      | 83      |
| SDSA | ソフトウェア開発の各プロセスにおけるセキュリティ評価 | 129           | 148     | 169     |

注: 略語説明 CRT (Communication Robustness Test), FSA (Functional Security Assessment), SDSA (Software Development Security Assessment)



通信路からの被攻撃中あるいは攻撃終了後に、あらかじめ定義された必須サービス（制御演算の継続など）が維持されることを実機テストによって検証する。具体的には、対象装置とHMI（Human-machine Interface）装置をネットワークで接続し、HMI装置でのデータ表示状態とPI/O（Process Input/Output）からの制御出力によって必須サービスの維持を検証する。

FSA（Functional Security Assessment）は、対象装置がシステムのセキュリティ機能面の要件を満たしているか否かを実機によるテストとドキュメントによって検証する。

SDSA（Software Development Security Assessment）は、セキュリティ要求仕様としてセキュリティ脅威モデルを策定し、その脅威に対してソフトウェア開発のライフサイクル全般にわたって設計・レビューされているか否かをドキュメントによって検証する。

### 5.3 情報制御ネットワーク用セキュリティ製品

情報制御システムは、長期の運用や設備・機能の拡張などにより、システムの運用開始後も装置の改変が発生するため、新旧装置が混在することが多い。そのため、単体でのセキュリティサポートをしたコンポーネント単体を導入するだけでは、セキュリティを維持することは困難である。

外部からの攻撃を侵入阻止するFWやIDSだけでなく、装置構成の変化を監視してネットワークに接続可能な装置を識別し、不要なコンポーネントの接続を遮断すること、または、攻撃や汚染を早期に検知して対応することが有効と考えている。例えば、日立グループが提供している不正端末接続監視を行うNX NetMonitorは、ネットワーク内を常時監視し、不審な装置が検出された場合には、セキュリティ運用システムに警告を発することができる。

## 6. 現場のインテリジェント化を推進する 耐環境小型コンピュータ

### 6.1 現場システムのインテリジェント化に対する要求と取り組み

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には、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ため、現場のインテリジェント化への取り組みを推進している。このためには、各種の通信環境に対応するほかに、現場情報を処理できる電子機器・情報機器を、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させる必要がある。

例えば、列車の車上表示システムでは、リアルタイム性と正確さが必要な旅客案内情報のほか、ニュース、広告、

天気予報など、乗客に提供する情報が多様化している。このシステムでは、多様な表示データを処理する小型コンピュータを「現場」である列車天井の裏側のスペースに設置する。したがって、そこで用いられる小型コンピュータには、小型であることと同時に、列車留置中の高温や低温・雨天時の結露、列車運行中の振動といった過酷な環境での動作が要求される。

このほか、スマートグリッドで用いる電力監視装置は、温度・湿度条件が厳しい屋外の電柱上部や、電氣的ノイズが強い変電機器設備の近辺に設置される。産業用ロボットの制御装置は、振動が大きく、硫黄などを含む腐食性ガスや塵埃（じんあい）の多い製造現場で運用される。また、電力監視装置や産業用ロボットの制御装置などは、据付けや交換作業が困難な設置環境にあるため、長期間安定して動作することが重要となる。現場のインテリジェント化による設置環境の拡大に伴い、耐環境性の要求も多様化している。

### 6.2 耐環境小型コンピュータの開発

これまで、前述の車上表示システム向け小型コンピュータや変電所向けの組み込みコンピュータを開発してきた。現在、耐環境性のニーズの高まりと多様化に応えるため、以下の7点に対応する耐環境小型コンピュータの開発に着手している。

- (1) 広い温度環境（-10～+60℃）への適合
- (2) 幅210 mm、高さ70 mm、奥行き225 mmのコンパクトサイズ
- (3) 耐環境密閉構造
- (4) 24時間365日連続稼働で10年の長寿命
- (5) ファンレス（自然空冷）による部品の定期交換の排除
- (6) HDD（Hard Disk Drive）レスによる耐振性強化
- (7) メモリECC（Error Check and Correction）による高信頼性

環境条件の厳しい現場に設置される高信頼制御装置〔制御用コントローラ、PLC（Programmable Logic Controller）など〕では、これまでメモリECC機能を独自のASICで実現してきた。

今回開発する耐環境小型コンピュータでは、近年、急速に普及が進んでいる小型・低消費電力の高性能SoC（System on a Chip）に注目し、メモリECC機能を備えるSoCを採用した。密閉構造に対応した低発熱化のため、プロセッサ部とメモリECC機能部をワンチップ化し、小型化と低消費電力化を図った。これに加え、部品レイアウトについて自然空冷条件下での熱流体解析検証を行い、ヒートスポットの発生を抑制するとともに、金属筐（きょう）体を独自

に最適化してSoCの発熱を接触放熱させることなどにより、10年寿命を踏まえた熱対策を行った。これらにより、ファンレス化と密封構造、および10年寿命を両立した。

振動が大きい環境での安定した動作を実現するため、ファイル装置にはCFast<sup>®</sup>カードを採用し、振動や衝撃に脆弱なメカニカル部を排除した。また、CFastスロットを含め、保守作業で手を触れるコネクタやLED (Light-emitting Diode) はすべて前面に配置し、取り付け・交換作業やケーブル抜おおよび表示確認などにおける保守性を高めた(表2、図10参照)。

※) CFastは、CompactFlash Associationの商標である。

表2 | 耐環境小型コンピュータの仕様

開発した耐環境小型コンピュータの主要仕様を示す。

| 項目          | 仕様  |  |
|-------------|---|--|
| プロセッサ (SoC) | インテル <sup>*1</sup> Atom <sup>*1</sup> プロセッサ (1.46 GHz) (コア数/スレッド数: 1/1) |  |
| メモリ         | メインメモリ  | DDR3L-SDRAM, ECC付き, 2 Gバイト                                     |
|             | 不揮発性メモリ   | MRAM, 512 Kバイト   |
| グラフィクス      | コントローラ  | SoC内蔵  |
|             | グラフィクスメモリ   | メインメモリと共有  |
|             | 表示解像度   | 最大解像度: 2,560×1,600 (WQXGA)                                     |
|             | 表示色   | 色数: 1,670万色 (24 bpp)   |
| ファイル装置      | CFastスロット   | CFastスロット×1 (フロント交換可)  |
|             | ディスプレイ  | Display port×1ポート  |
| 入出力インタフェース  | USBポート  | 1ポート (USB3.0準拠, USB Aタイプコネクタ)<br>3ポート (USB2.0準拠, USB Aタイプコネクタ) |
|             | LANポート  | 3ポート (1000 Base-T, Wake-on-LAN対応)                              |
|             | RAS機能   | LED, WDTなど   |
| サポートOS      | 日立カスタマイズLinux <sup>*2</sup> (予定)  |  |
| BIOS        | EFI   |  |

注: 略語説明ほか SoC (System on a Chip), DDR (Double-Data-Rate), SDRAM (Synchronous Dynamic Random Access Memory), ECC (Error Check and Correction), MRAM (Magnetoresistive Random Access Memory), WQXGA (Wide Quad Extended Graphics Array), bpp (bits per pixel), LAN (Local Area Network), RAS (Reliability Availability and Serviceability), LED (Light-emitting Diode), WDT (Watchdog Timer), BIOS (Basic Input/Output System), EFI (Extensible Firmware Interface)

\*1 インテル, Atomは, 米国およびその他の国におけるIntel Corporationの商標である。

\*2 Linuxは, Linus Torvalds氏の日本およびその他の国における登録商標あるいは商標である。



図10 | 耐環境小型コンピュータの外観

ケースは放熱性に優れた独自の金属筐(きょう)体とした。コネクタとLEDを前面に配置し、保守性を高めている。

## 7. おわりに

本稿では、社会インフラの長期安定稼働と高可用性を支える情報制御システムの最近の課題と技術開発の内容を紹介した。情報制御システムに最新のITを積極的に導入するとともに、積み上げてきたノウハウを活用し、変化の激しいITとサービス拡張の要請に対して、社会インフラの安全・安心を支えるための技術課題を解決する。

日立グループは、さらに安全・安心で高品質な社会インフラをめざし、今後も技術開発を進めていく。

### 参考文献

- 1) 水野: ビッグデータによる経済・社会現象の統計分析と経済物理学, 研究報告知能システム (ICS), 2014-ICS-173 (4), 1-3 (2014.1)
- 2) 清野: 仮想化の基本と技術, 翔泳社 (2011)
- 3) IEC 61508 2nd edition: Functional safety of electrical/electronic/programmable electronic safety-related systems (2010.4)

### 執筆者紹介



#### 清水 勝人

日立製作所 インフラシステム社 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, 情報制御システム向けのサーバとコントローラの開発・設計に従事



#### 西島 英児

日立製作所 横浜研究所 情報プラットフォーム研究センター ソフトウェアプラットフォーム研究部 所属  
現在, 社会インフラ向けソフトウェアプラットフォームの研究開発に従事  
電気学会会員, 情報処理学会会員



#### 大平 崇博

日立製作所 インフラシステム社 制御プラットフォーム開発本部  
システム技術開発部 所属  
現在, 情報制御システムのミドルウェア開発に従事



#### 大久保 訓

日立製作所 インフラシステム社 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, 情報制御システムのセキュリティ開発に従事



#### 西村 卓真

日立製作所 インフラシステム社 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, 情報制御システムのコンポーネント開発に従事



#### 清水 俊樹

日立製作所 インフラシステム社 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, 情報制御システムのコンポーネント開発に従事