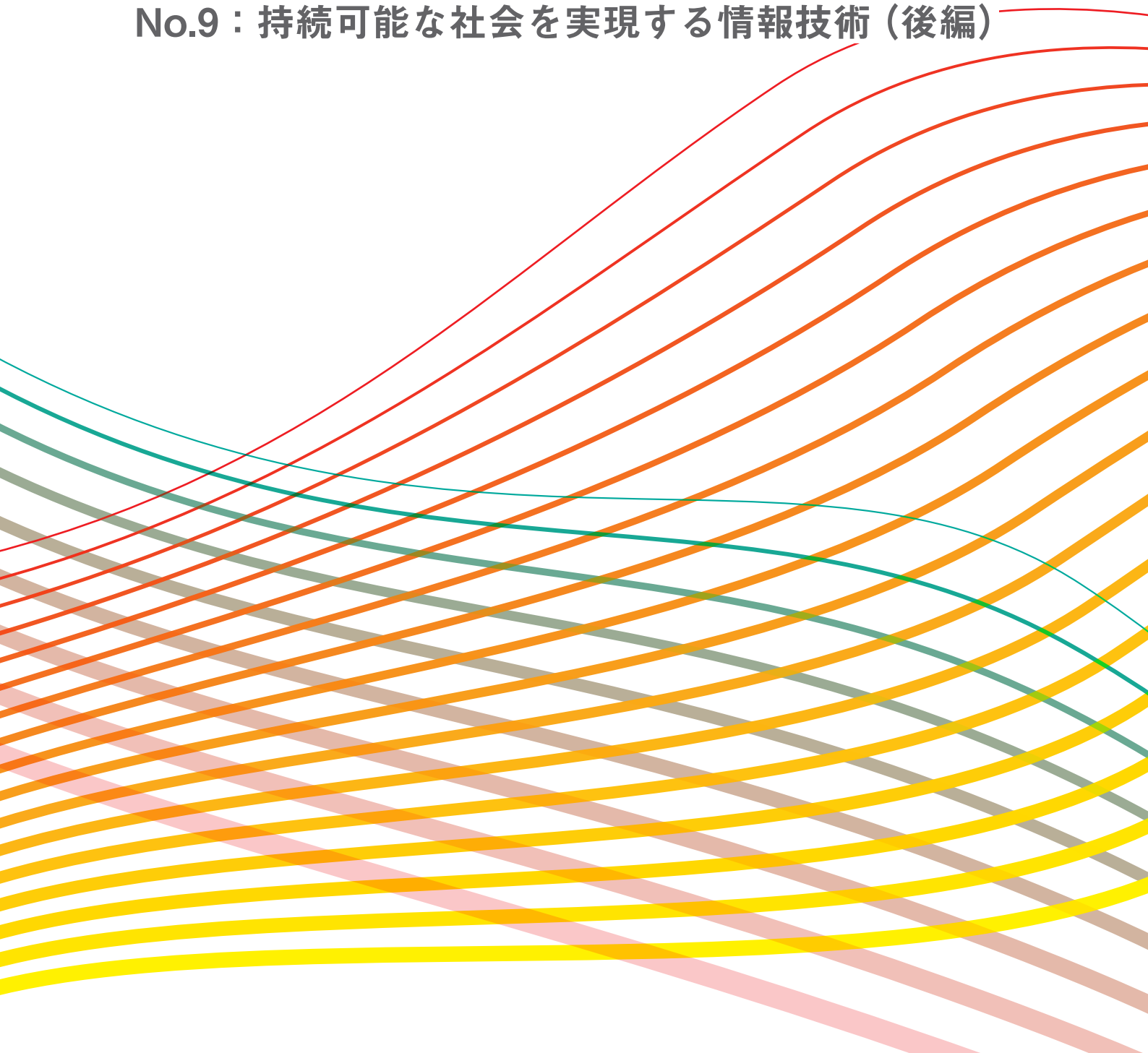
三菱電機技報　96巻8,9号（通巻1092号）　ISSN 0369-2302／CODEN:MTDNAF

MITSUBISHI ELECTRIC
Changes for the Better

三菱電機技報

8-9
2022
Vol.96 No.8-9

No.8：持続可能な社会を実現する情報技術（前編）
No.9：持続可能な社会を実現する情報技術（後編）



三菱電機では，サステナビリティ経営を実現する４つのビジネスエリアとして，「インフラ」「インダストリー・モビリティ」「ライフ」「ビジネスプラットフォーム」を設定しています。

三菱電機技報ではこの４つのビジネスエリアに分類し特集を紹介しています。

今回の特集では全エリアを支える基盤となる“持続可能な社会を実現する情報技術（前編・後編）”（８・９月号）をご紹介します。

目 次 Contents

三菱電機技報 Vol.96 No.8,9 2022

No.8

特 集 持続可能な社会を実現する情報技術(前編) Information Technologies for Realizing Sustainable Society

No.9

特 集 持続可能な社会を実現する情報技術(後編) Information Technologies for Realizing Sustainable Society

松浦陽平*
Yohei Matsuura

統合IoT“ClariSense”設計ガイド

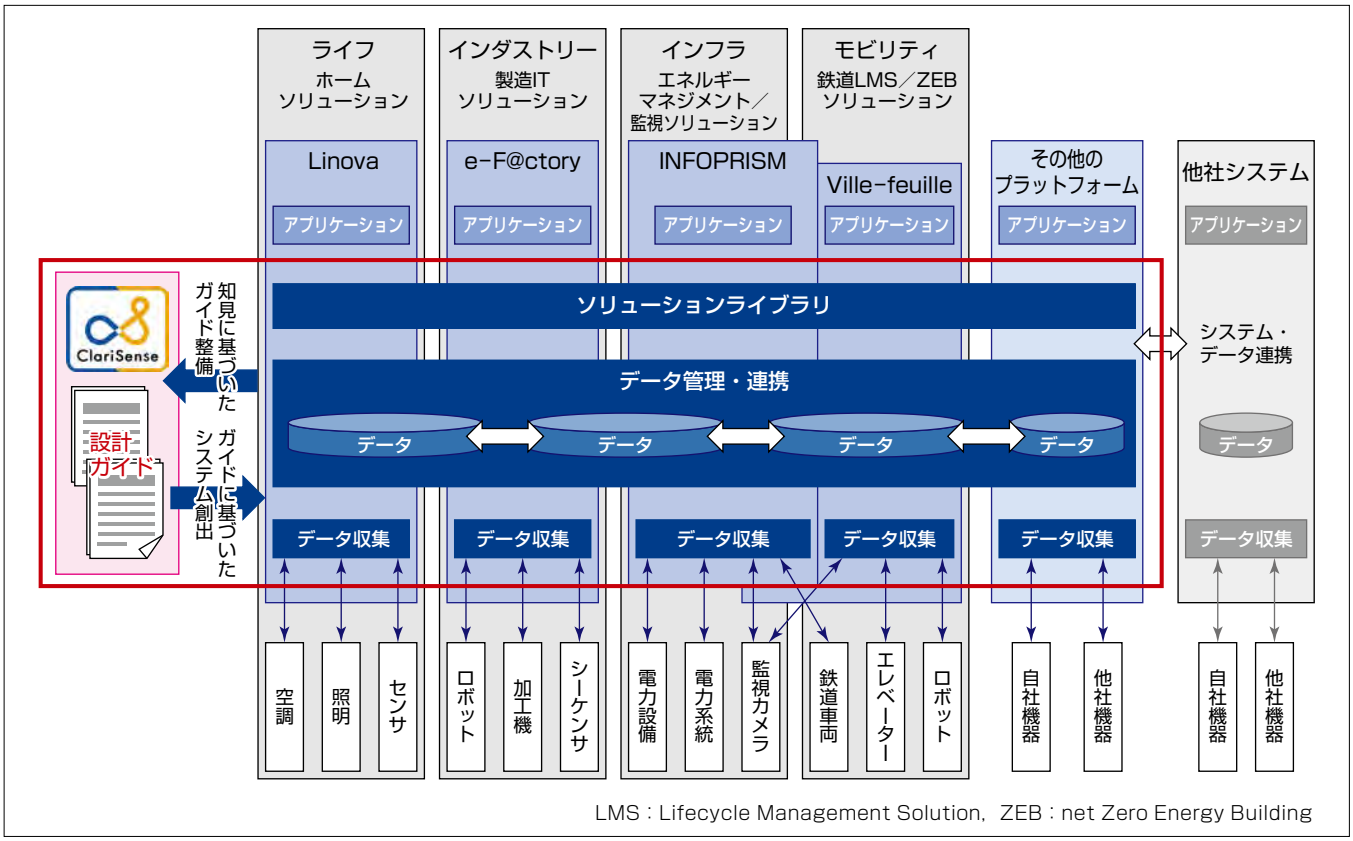
Introduction of Internet of Things Suite "ClariSense" Design Guides

要　旨

現在，事業DX(Digital Transformation)の実現に向けて，様々な分野でIoT(Internet of Things)システムの活用が進んでおり，国内市場規模は2025年には10.2兆円を超えると予測されている。三菱電機では，ライフ，インダストリー，インフラ，モビリティの各分野で，当社が強みとする機器，AI技術“Maisart(マイサート)”，セキュリティなどの技術資産を活用したIoTソリューションを提供しており，この活動を通して得た知見を統合IoT“ClariSense(クラリセンス)”の設計ガイドにまとめている。設計ガイドは，IoTアーキテクチャ定義書，IoTシステム設計ガイド，マイクロサービス設計ガイド，API(Application Programming Interface)設計ガイド，ネットワーク設計ガイド，DevOps(注1)構築ガイドで構成しており，IoTシステムを構築する上で考慮すべき点や事例を記載した。これらのガイドを当社内で一元的に整備し共有することで，各領域の既存IoTプラットフォームの強化や，新たなIoTシステムの開発効率化，システム間連携による，新たなIoTソリューション創出の迅速化を実現する。

ClariSenseの設計ガイドは，今後も柔軟で拡張性の高いIoTプラットフォーム／IoTシステム／IoTソリューションを迅速に創出するために，各領域のIoTプラットフォームや個別のIoTシステムの構築を通して得た知見及びITの最新技術を継続的に取り入れていく。

(注1)　開発担当者と運用担当者が連携して協力する開発手法を指す造語。



LMS：Lifecycle Management Solution，ZEB：net Zero Energy Building

ClariSenseと既存IoTプラットフォームの関係

当社では，ライフ，インダストリー，インフラ，モビリティの各分野で，IoTシステムを活用したソリューションを提供している。ClariSenseでは，既存IoTプラットフォーム構築で得た知見を設計ガイドとして整備するとともに，新規IoTプラットフォームの迅速な構築や，IoTプラットフォーム間の効率的な連携を可能にする。

*情報技術総合研究所

1. ま え が き

DXの実現に向けて，様々な分野でIoTシステムの活用が進んでいる。IoTシステム向け事業は今後も拡大を続けて，**図1**に示すように2025年には国内市場規模は約10.2兆円になると予測されている(1)。本稿では，現在整備を進めている設計ガイドについて述べる。

2. IoTシステムに対する取組み

2.1 IoTシステムの構成要素の整理

IoTシステムを構成する基本的な構成要素を**図2**に示す。

(1) データ収集・蓄積系機能

機器が生成，保持しているデータを収集，蓄積し，アプリケーションに渡す。

(2) 制御系機能

アプリケーションやデータ収集・蓄積系機能のイベントトリガーによって機器を制御する。

(3) 運用系機能

接続された機器に対して認証を含む運用・管理，ユーザー／管理者／他システムに対する認証管理，各機能要素の設定管理を行う。

(4) アプリケーション

データに基づく分析・処理，処理に基づく制御指示，ユーザー／管理者／他システムへのデータ提供・画面表示や制御指示の受付を行う。

(5) 広域ネットワーク

インターネットや，組織内で利用されるイントラネットを指す。IP(Internet Protocol)網をベースに，通信頻度やデータサイズに応じてプロトコルを選択する。

(6) エッジ機器

機器から伝送されたデータを一定期間又は機器からデータ取得完了したタイミングで，サーバとネットワークに合わせたプロトコルに変換する。要件に応じてデータの暗号化やカプセル化処理を行う。

(7) 機器

機器内部や周囲の様々な物理的・化学的な特性(温度，湿度，pH等)をセンサでデジタル化・データ化し，伝送で利用されるネットワークに合わせてプロトコル変換が行われ，通信モジュールから他構成要素へ伝送する。

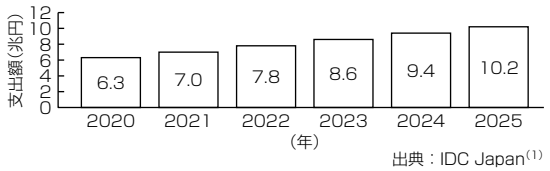


図1．国内IoT支出額予測 2020年～2025年

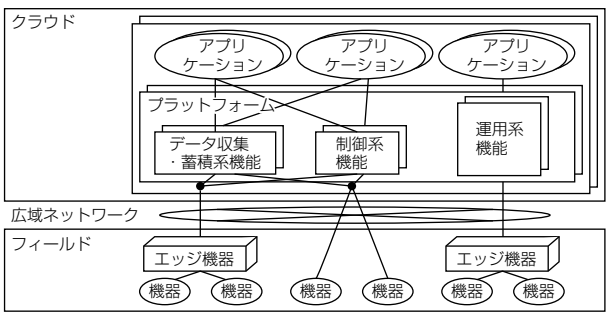


図2．IoTシステムの構成要素

2.2 各事業分野での取組み

多様化する社会課題の解決に向けて，ライフ，インダストリー，インフラ，モビリティの各分野で，IoTシステムを活用したソリューションを提供している。

2.2.1 ラ イ フ

2019年から，インターネットを介して当社IoT家電のデータを収集・管理する基盤として，グローバルIoT共通プラットフォーム“Linova”を提供している(2)。2020年には，家電統合アプリケーション“MyMU”をリリースし，Linovaで管理している複数の家電を横断的に制御できる仕組みを顧客に提供している。

2.2.2 インダストリー

2003年から，生産現場向けにFA-IT統合ソリューション“e-F@ctory”を提供している(3)。また，Edgecross(注2)コンソーシアムの活動にも力を入れている。同コンソーシアムは，エッジコンピューティング領域で，機器や通信規格の違いを超えてつながり，データの収集と活用が容易になるようなオープンなプラットフォームを作り，企業や産業の枠を超えた新たな付加価値の創出を目指している。

(注2) Edgecrossは，一般社団法人 Edgecrossコンソーシアムの登録商標である。

2.2.3 イ ン フ ラ

2017年から，社会・電力インフラ設備の運用・保全業務の効率向上に貢献するIoTプラットフォームとして，“INFOPRISM”を提供している(4)。INFOPRISMは，発電機などの設備保全システム，公共施設などの統合監視システム，上下水道などの設備運用最適化システムなどに適用されている。2020年からは，ビル内設備の稼働データやセンシングデータなどを収集・蓄積し，AIやビッグデータ解析などの技術を活用してデータ処理を行うIoTプラットフォームとして，“Ville-feuille”を提供している(5)。

2.2.4　モビリティ

2019年から，鉄道車両の様々な情報をリアルタイムに収集・分析するIoTプラットフォームとして，“鉄道LMS on INFOPRISM”を提供している。また，2020年から，ビル内ダイナミックマップを用いて，清掃・警備・配送・案内用サービスロボットや次世代型電動車椅子などのパーソナルモビリティの各種モビリティと，エレベーターや入退室管理システムといったビル設備を連携制御するサービスをVille-feuille上に構築している。

3．ClariSenseでの設計ガイド

ClariSenseは，**2章**で述べたような各事業分野でのIoTシステムに対するセキュリティ，ネットワークなどに関する知見や技術資産を，設計ガイドやソリューションライブラリとして整理したもので，当社グループ内で共有・活用を推進している[6]。これによってIoTシステムの設計の効率化や，事業分野を横断した新たなIoTシステムソリューションの実現を目指す。ClariSenseの設計ガイド構成と，各設計ガイドで扱う記載内容について述べる。IoTシステムの構成要素との対応関係を**図3**に示す。

3.1　IoTアーキテクチャ定義書

当社で推進しているIoTシステム構築に関わる異なるバックグラウンドを持つステークホルダーが，共通認識に基づいて議論するための土台になるIoTシステムの機能要素とAPIの考え方を中心に記述したものである。

IoTシステムのアーキテクチャに関して，様々な団体でリファレンスアーキテクチャを定義しているが，ClariSenseではIIC(Industry IoT Consortium)で策定しているIIoT(Industrial IoT)向けリファレンスアーキテクチャのIIRA(Industrial Internet Reference Architecture)を参照している。IIRAは当社も策定に関与しており，2019年6月に策定されたv1.9が最新版である。

3.2　IoTシステム設計ガイド

開発目的に応じて，機能とコストを両立させるためのクラウド上のマネージドサービスの選定方法や，サービス化後の運用時でのサービスレベル管理・監視設計などを整理したガイド集である。IoTシステム設計ガイドは全7分冊の構成で，**図4**に示すように各分冊は本編と付録で構成している。本編では，IoTシステム設計時の確認項目を示したチェック項目とその考え方，社内でのシステム構成例を事例として紹介した。

(1) 概要編：ClariSense設計ガイドの総括，ガイド体系の説明，場所事例の一覧を紹介した文書
(2) データ管理編：データ形態・利用方法等を考慮した要件に合わせたサービスの選定と，データ管理に必要な項目を紹介した文書
(3) データ連携編：データ連携に使用する技術・製品を選択するために確認すべき項目をまとめるとともに，連携対象のデータ発見や利用に有用なメタデータの例を説明する文書
(4) セキュリティ編：IoTシステムへ実装することが想定される典型的なセキュリティ機能の設計方法を示した文書。本編はさらにクラウドベンダーごとに分冊を提供(セキュリティ編分冊-AWS(注4)-，セキュリティ編分冊-Azure(注5)-)

PDF：Portable Document Format
（注3） Excelは，Microsoft Corp.の登録商標である。

図4．IoTシステム設計ガイド各編の構成

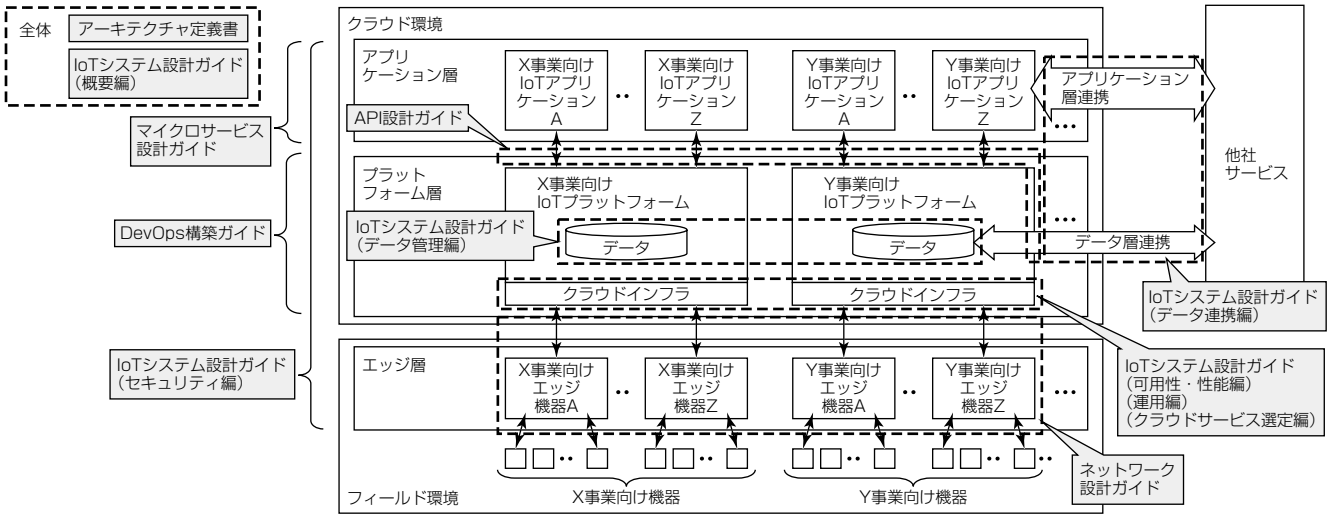


図3．IoTシステムの構成要素との対応関係

(5) 可用性・性能編：IoTシステムを構築するために利用するクラウドサービスに対して，非機能要求として求められる可用性・性能として考慮すべき観点をまとめた文書
(6) 運用編：ITサービス設計で，分散トレーシング等，運用設計に関わる文書
(7) クラウドサービス選定編：クラウドサービス(特にPaaS(Platform as a Service))について，要件に合わせたサービス選定の進め方をまとめた文書

(注４) AWSは，Amazon Technologies, Inc.の登録商標である。
(注５) Azureは，Microsoft Corp.の登録商標である。

3.3 マイクロサービス設計ガイド

マイクロサービスは，個々に開発された複数の小さなサービスを連携させて管理，運用するソフトウェアアーキテクチャである。マイクロサービスは，ビジネス変化への柔軟な追従や，サービスの再利用性向上に有効な手段である一方，導入を適切に行うためには，設計上の留意点を正しく理解する必要がある。このガイドでは，マイクロサービスがどのような局面で何を解決するのか，設計するに当たってどのようにサービスを分割するのか，どのようなエンジニアリング手法で開発を行うのかなどを整理している。新規システム開発と，モノリシックなシステムからの移行開発の二つの開発パターンに対して，考慮すべき事項をまとめるとともに，マイクロサービス設計手法，アジャイル開発プロセス，開発のベストプラクティスを記載している。

3.4 API設計ガイド

社外システム連携を前提に，主にアプリケーション層連携，プラットフォーム層連携で，セキュリティ，ID連携等も考慮した疎結合型でのデータのやり取りを行うためのWeb APIの考え方をまとめた文書である。具体的には，APIの設計としてエンドポイントの命名規則やレスポンスフォーマットに関する注意事項，実装として，AzureやAWS等のパブリッククラウドサービスでの構成例，運用として利用状況の管理やバージョン管理方式についてまとめている。

3.5 ネットワーク設計ガイド

フィールドネットワーク上のデータを，広域ネットワーク(IP網)を介して収集する場合に必要となるプロトコル変換及びデータ変換についてまとめたものである。このガイドは，事業分野に依存しない共通的な基本設計手法をまとめた総括編と，ユースケースごとのプロトコル変換・データ変換の実現例を記載した個別編から構成される。

3.6 DevOps構築ガイド

DevOpsを実践するために必要になるシステム環境の設計の考え方及び事例を示す文書であり，導入編，AWS実践，Azure実践の分冊から構成される。このガイドでは，バージョン管理方式やブランチ方式，CI/CD(Continuous Integration/Continuous Delivery)のパイプラインの設計方式についてまとめるとともに，運用でのモニタリングの考え方，モニタリング結果の開発へのフィードバックの考え方についてまとめている。

4. ClariSense設計ガイドの深化に向けて

4.1 設計ガイドコンテンツの拡充

従来のように，全体像を描いて，その中のミッシングピースを埋めていくような取組みスタイルでは，進化の早いIoTシステムではニーズのないガイドを生み出すことになるとともに，コンテンツの陳腐化を早めることになる。社内外のニーズを常にウォッチし，記載するコンテンツを取捨選択するような柔軟な管理を行っていく。

4.2 設計ガイドの共有

現在は作成した設計ガイドを社内配布しているが，迅速にニーズを取り込むため，社内で活用されているコンテンツ管理システムとの連携を計画している。これによって，執筆者に対する直接的なフィードバックや，利用者がウェブブラウザ経由で直接設計ガイドを執筆することによる更なる知見蓄積の加速が期待できる。

5. む す び

当社が強みとするコアコンポーネントに，豊富なフィールドナレッジやIoTシステム構築ノウハウを掛け合わせて得た知見を一元的に整備し，当社グループ内で共有するClariSense設計ガイドについての取組みを述べた。

今後も設計ガイドを活用し，柔軟で拡張性の高いIoTソリューションを迅速に創出していく。

参 考 文 献

(1) IDC Japan：国内IoT市場支出額予測（2021）
https://www.idc.com/getdoc.jsp?containerId=prJPJ47587321
(2) 櫻井翔一朗：“暮らし空間イノベーション”を実現するグローバルIoT家電サービス，三菱電機技報，**94**，No.10，566～569（2020）
(3) 水落隆司：FA-IT統合ソリューション“e-F@ctory”を支える最新のFA技術・システム，三菱電機技報，**93**，No.4，216～221（2019）
(4) 廣岡俊彦：社会・電力インフラIoTプラットフォーム“INFO-PRISM”，三菱電機技報，**93**，No.7，397～400（2019）
(5) 石井周作：三菱電機のスマートビルソリューション，三菱電機技報，**94**，No.5，264～268（2020）
(6) 鶴　　薫：IoTソリューションを迅速に創出する統合IoT“Clari Sense”，三菱電機技報，**95**，No.4，276～279（2021）

特集論文

ブロックチェーン技術を活用したデータ共有管理技術

山田将史* Masafumi Yamada
楓　仁志* Satoshi Kaede
松本光弘† Mitsuhiro Matsumoto
横地　洋* Hiroshi Yokochi

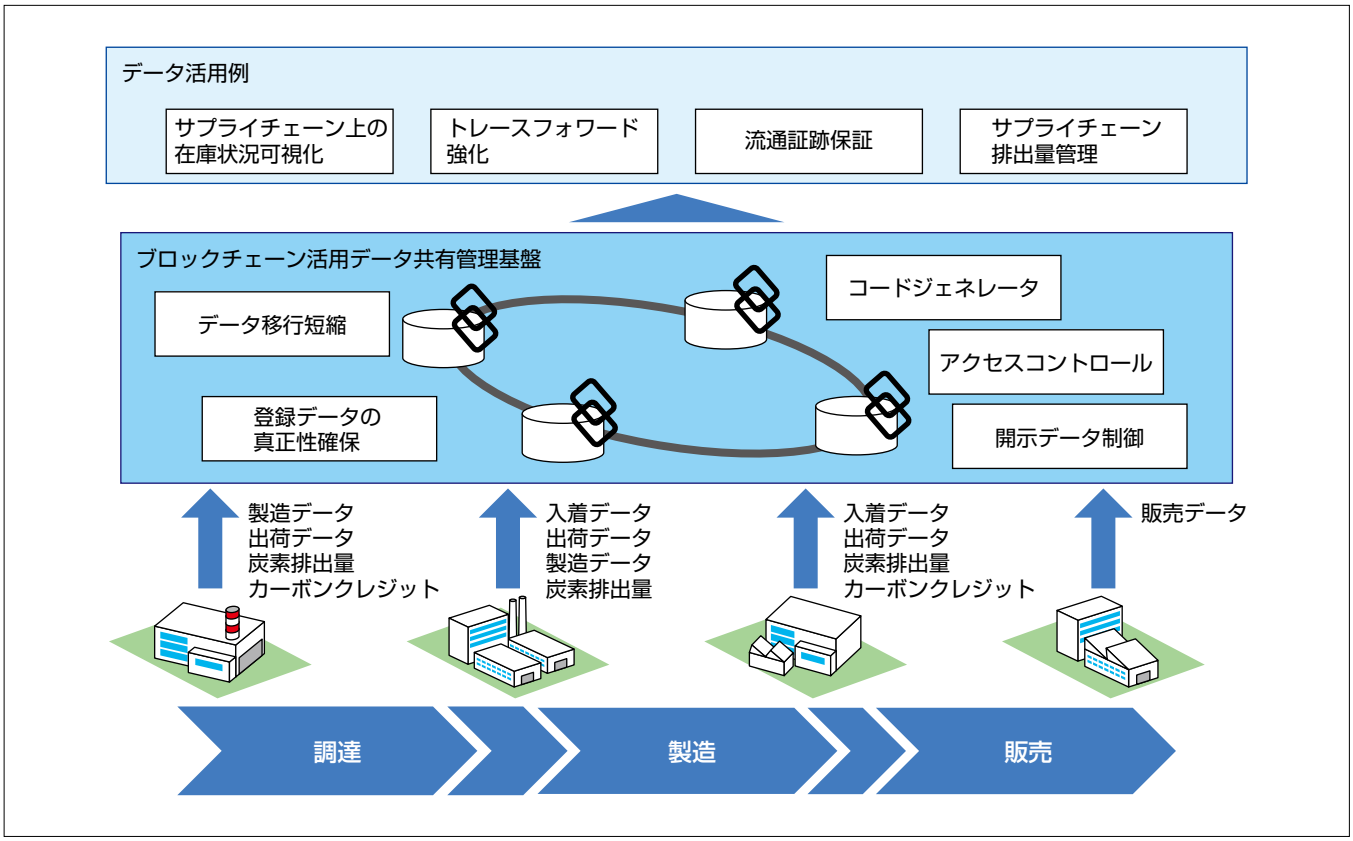
Data Sharing and Management Technology for Multi－Stakeholders based on Block－Chain

要　旨

デジタルトランスフォーメーション(DX)の取組みが社会的に進んでおり，DXを進展させるための様々な技術開発が行われている。DX実現での重要な要素はデータの扱いであり，特に複数の事業体間でのデータ共有と活用の取組みでブロックチェーン技術の活用検討が活発化している。ブロックチェーンを活用した複数ステークホルダー間でのデータ共有管理の取組み例には，サプライチェーン情報の共有，モノと情報の関連性管理，ステークホルダー相互のデータ共有による新たな価値創出などがある。

三菱電機では，複数のステークホルダーで協調して新たな価値を創出することを目的として，ブロックチェーンを活用した複数ステークホルダー間データ共有・管理技術の研究開発を行っている。例えば，①登録時の誤り・不正データの混入防止技術，②ブロックチェーン上のデータに対するアクセスコントロール技術と開示データ粒度制御技術，③ブロックチェーン活用システムの開発支援・運用支援技術，④ブロックチェーン上のデータ活用技術などである。

今後も，複数ステークホルダー協調によるDXを支えるデータ共有管理技術とその社会実装に必要なブロックチェーン活用の技術開発を進めて，持続可能な社会実現への貢献に向けて取り組んでいく。



ブロックチェーンを活用したステークホルダー間データ共有・管理のサプライチェーンへの適用イメージ

サプライチェーンをユースケースとした，ブロックチェーンを活用したステークホルダー間データ共有・管理への適用イメージを示す。複数のステークホルダー間で，各社が他ステークホルダーと，各データの説明性，追跡可能性，透明性，アクセス性を確保するための技術とデータを共有することによるデータ活用例を示す。

*情報技術総合研究所　†同研究所(博士(情報科学))

1. まえがき

DXの取組みが社会的に進んでおり，DXを進展させるための様々な技術開発及び社会実装が行われている。DXでは，個社に閉じた変革ではなく，複数のステークホルダーと協調して新しい価値を創出・提供するという取組みが重要である。

DX実現での重要な鍵の一つはデータである。これは，DXでは，データに基づいた判断と行動が増加するとともに，各事業体が持つサービスやシステムが相互に接続して大きな系(System of Systems)を成すことが増えてきているためである。このとき，システムが出力する結果やシステムが扱うデータに対して，説明性(Accountability)，追跡可能性(Traceability)，透明性(Transparency)，アクセス性(Accessibility)が求められる。そのため，様々な機器・システムが生み出すデータをいかに管理するか，管理して活用するかが非常に重要である。

本稿では，複数ステークホルダー間でデータ共有・管理する技術として注目されているブロックチェーン技術について，当社の研究開発技術例，活用ユースケースと今後の展望について述べる。

2. ステークホルダー間データ共有・活用の動向

内閣府の第5期科学技術基本計画で，Society 5.0が提唱され，“経済発展と社会的課題の解決を両立する，人間中心の社会を実現するための，サイバー空間とフィジカル空間を高度に融合させたシステム”への取組みが進められている。産業界では，サプライチェーンのDXを重要な課題の一つとして捉えて，サプライチェーン上複数ステークホルダーにまたがるデータ共有管理とデータ活用による“品質・トレーサビリティの向上”や“在庫状況の的確な把握と不測事態に対する迅速かつ柔軟な対応”への取組みが提言されている[(1)]。産業界での具体的な取組みを述べる。

国際半導体製造装置材料協会(SEMI)では，“Equipment and Material Traceability”の業界標準化活動を行っている。対象は，“半導体デバイスの製造・流通を管理するトレーサビリティ”“半導体製造装置・サブシステムを管理するトレーサビリティ”や“半導体デバイスを構成する部材を管理するトレーサビリティ”などが挙げられており，ブロックチェーンを活用して業界内でのデータ共有管理による説明性，追跡可能性，透明性確保に向けた取組みが進められている。

自動車産業でも，Mobility Open Blockchain Initiative(MOBI)が，車両アイデンティティ(VID)を個別自動車判別のためのユニークな識別子としてブロックチェーン・分散台帳上で管理し，所有者，保証，走行距離や製造証明書などの重要な情報と紐(ひも)付けて管理する仕組みの規格化を行っている。このほかにもVIDを軸にした炭素クレジットのトークン化，サプライチェーン情報の共有，新たなサービス創出に向けた取組みを複数事業体連合で進めている。

さらに，カーボンニュートラルを目指す動きが世界的に加速している中，サプライチェーン排出量管理の動きも進んでいる。サプライチェーン排出量は，自社での“燃料の燃焼”や“電気の使用”だけではなく，自社の上流・下流での事業活動に関係するあらゆる排出を合計した排出量であり，自社以外の事業者との連携強化が不可欠になってきている。

これらの取組みのように，業界内複数ステークホルダー間や業界をまたいだステークホルダー間でのデータ共有・管理と，そのデータを活用した付加価値創出の取組みが活発化しており，中でもデータの説明性・追跡可能性・アクセス性・透明性の確保のためにブロックチェーン技術を活用する取組みが増えている。**3章**以降では，当社での，ブロックチェーンを活用したステークホルダー間データ共有・管理のための研究開発の取組みについて述べる。

3. ブロックチェーンを活用したステークホルダー間でのデータ共有・管理技術

ブロックチェーンは，ブロックチェーンネットワーク上で発生するトランザクションをデータの塊(ブロック)として扱い，その際に一つ前に記録されたブロックのハッシュ値とともに時系列順に記録する。このデータ構造自体やスマートコントラクト，コンセンサスアルゴリズム，暗号技術，分散型台帳管理という技術の組合せによって，データの透明性，説明性，追跡性の確保につながっている。

一方，ブロックチェーンでは登録される時点のデータ自体に誤りがないことや不正な内容ではないことの保証は難しい。また，ブロックチェーンに登録する情報は，ブロックチェーンネットワーク上の全ノードで記録され，登録情報がブロックチェーンネットワークへの参加者に公開される。そのため，一部データを一部参加者にだけ開示可能にしたいなどのビジネス上の機微な情報の扱いに工夫が必要である。さらに，複数ステークホルダーでデータをブロックチェーン上で共有管理するシステムでは，長期間にわたるシステム運用の観点では，開発効率化やシステム更新手段の整備が重要である。

この章では，これら複数ステークホルダー間でのデータ共有基盤としてブロックチェーンを活用する際の課題解決を目的とした当社技術開発の事例を述べる。

3.1　登録データの誤り・不正データ混入防止

ブロックチェーン分散台帳上に記録されたデータは，耐改ざん性に優れているが，記録しようとしているデータに誤りがないこと自体の担保は難しい。

そのため，分散台帳に記録されるデータに誤りや不正がないことを検証するスマートコントラクトを準備し，データ操作時の誤り・不正データの混入を防止する。開発したデータ検証スマートコントラクトの検証項目には，“データ形式：入力データはフォーマットにのっとっているか”“履歴データからの一貫性：入力データは過去データと比較して矛盾していないか”“データ同士の関係性：入力データは外部データを含む他データとの関係性が正しいか”などがあり，それぞれのルールに準拠しているデータ操作のリクエストであることを検証した後に，トランザクションとして実行する。

また，データ検証スマートコントラクトを用途ごとに作成するのは負担になるとともに，開発したスマートコントラクトごとにそれ自体の誤りや不正がないことを確認することも運用上の負担になるため，“データ検証スマートコントラクトのテンプレート”と“検証項目のルールを記載したパラメータファイル”を入力とするコードジェネレータを開発し，運用面での負担緩和を実現した(**図１**)。

3.2　アクセスコントロールと開示データ粒度制御

先に述べたとおり，ブロックチェーン上でのデータ共有・管理では，一部データを一部参加者にだけ開示可能にしたいといったビジネス上の機微な情報の扱いが難しい。一部のステークホルダーで個別ネットワークを構成し，開示範囲を限定することは可能であるが，開示範囲ごとに個別ネットワークを管理する必要があり運用が困難になる。また，共有データの一部へのアクセス制御の実施も困難である。当社では，関数型暗号によって暗号化されたデータをブロックチェーン上に記録し，暗号化時に指定した権限を持つユーザーに参照権限を与えることで，データ・ユーザー単位に対して[(2)]，設定した複数の属性とユーザーロール定義をすることで，細かなアクセスコントロールを実現した(**図２**)。

また，データの開示範囲を抑制すると，参加するステークホルダー間で活用できる情報が少なくなるため，複数の保護対象データを集約して，データが持つ意味の粒度を粗くして公開することも有用である。例えば，サプライチェーンで，複数のステークホルダーが持つ在庫量を，ある地域での在庫総数のように表現することで，サプライチェーン全体での在庫最適化への活用などが考えられる(**図３**)。

3.3　ブロックチェーン間のデータ移行

システムの運用が長期にわたる場合，利用しているブロックチェーン基盤(Hyperledger Fabric[(注1)]，Ethereum[(注2)]等)によっては，バージョンアップに伴うシステム更新やデータ移行が必要なケースがある。ブロックチェーンデータは，過去のトランザクションデータを全て移行する必要があ

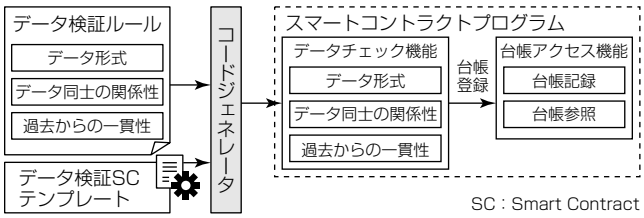


図１．データ検証スマートコントラクトの概念図

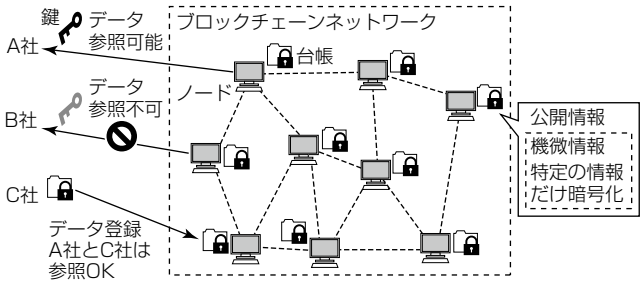


図２．ブロックチェーン上での特定情報への開示制御

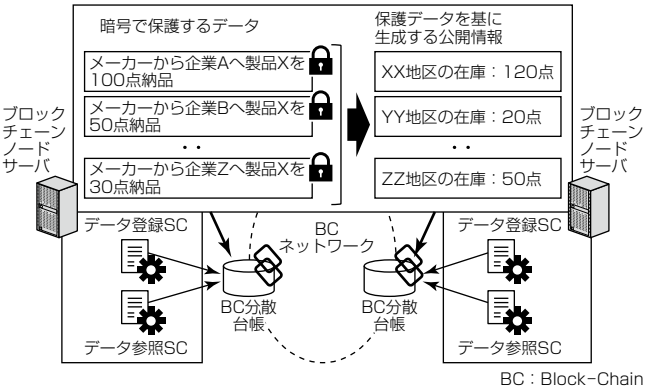


図３．公開データ粒度変更によるデータ共有の概念図

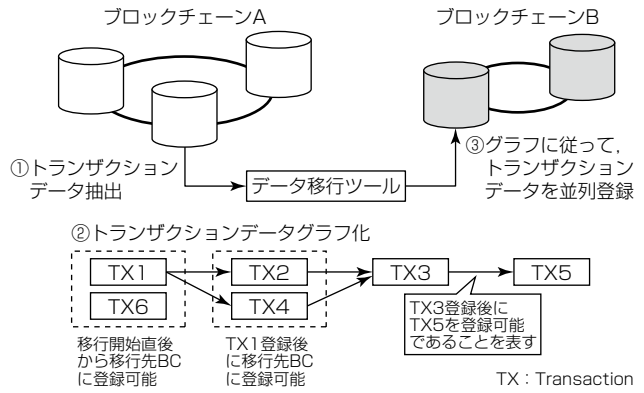


図４．データ移行効率化の概念図

るため，長期運用しているほど，移行対象のデータも多く，移行時間がかかる。

当社では，データ移行時間を短縮するために，トランザクション間の依存関係をグラフ化し，グラフ表現に基づいて依存関係がないトランザクションを並列登録する方式を開発した(**図４**)。

(注１) Hyperledger Fabricは，The Linux Foundationの登録商標である。
(注２) Ethereumは，Stiftung Ethereumの登録商標である。

4. ユースケース

３章までで，当社での複数ステークホルダー間データ共有・管理に向けたブロックチェーン活用技術を述べた。

この章では，この技術の適用によって効果が期待できるユースケースを述べる。

4.1 保守・アセット管理への適用

機器保守を行う業界では，保守業務効率化に向けて，デジタルアセット管理が注目されている。機器の保守業務には，定期的な稼働状態の検査や，機器の修繕，リプレース及びそれらの計画と結果の管理が含まれる。IoT(Internet of Things)技術の発達に伴い，保守業務やアセット管理業務は，様々な分野で機器の稼働データを使った状態基準の保守と，その結果の活用へと移行している。また，稼働データだけではなく，設計データ，製造データ，トレーサビリティデータと組み合わせて活用することで，トレースバック・トレースフォワードへの寄与や，リプレース時期の最適化などへの寄与も可能になる。

このように運用開始後も複数事業体にまたがって各社が持つ関連データを活用するための基盤として**３章**で述べたアクセスコントロール技術や開示データ制御技術などを組み合わせて，ブロックチェーンベース企業間デジタルスレッド技術を開発した。企業間デジタルスレッド技術は，対象とする機器の設計時から運用中，そして廃棄されるまでに創出される種々情報(設計データ，製造データ，トレーサビリティデータ，保守履歴データ，稼働データなど)を結び付けて管理する技術である。この技術によって，各データの管理場所によらず，対象の来歴の真実性を保持して，各種データを活用することで保守業務とアセット管理の高度化に寄与可能である。

4.2 サプライチェーンへの適用

製造業では，サプライチェーンでの“品質・トレーサビリティの向上”や“カーボンニュートラル”への取組みが始まっている。これらの取組みは自社だけで完結するものではなく，サプライチェーンに関わる複数ステークホルダーの協調による実現が求められる。これら取組みでの複数ステークホルダー間での信頼の置ける製品流通データの共有管理に，**３章**で述べた技術を組み込んだブロックチェーンを活用したデータ共有管理基盤の適用が考えられる。

このデータ共有基盤は，複数ステークホルダー間で，製品の流通情報と対象製品の関連情報(炭素排出量など)の正しさを担保して共有管理するとともに，ステークホルダーごとのデータアクセス制御を行うことで，データを安全に管理しながら透明性の高いトレーサビリティを実現する。

また，製品の流通データを活用することで，サプライチェーン全体の流通状況を反映した生産計画や在庫管理などへもつながる。

4.3 データ流通管理に向けた取組み

現在，異業種間のデータ共有やデータ流通の観点でのルールや仕組み作りが国内外で進んでおり[3]，当社でもデータ流通管理のための技術開発を行っている。この取組みでは，データ利活用での利用制御と証跡管理を可能にするデータ流通管理技術や，データの意味・構造を管理するためのデータカタログ管理の技術開発を行っている。また，データ管理基盤間のインターオペラビリティの観点も必要である。今後は，ステークホルダー間のデータ共有・管理に加えて，異業種間でのデータ共有やデータ流通に向けて，MaaS(Mobility as a Service)など複数の移動事業体間でのデータの相互利用やデータ共有の促進へ寄与するものとして取組みを進める。

5. むすび

本稿では，複数ステークホルダー間にまたがるデータ共有管理の重要性・有用性とブロックチェーン技術活用による実現に向けた例を，複数ステークホルダーの協調によるDX例とともに述べた。また，ブロックチェーン活用に関する当社技術開発の取組みとその活用ユースケース案を述べた。

今後も，持続可能な社会の実現への貢献に向けて，複数ステークホルダー協調によるDXを支えるデータ共有管理技術とその社会実装に必要なブロックチェーン活用の技術開発を進める。

参考文献

(1) 一般社団法人 日本経済団体連合会：Society 5.0時代のサプライチェーン (2020)
https://www.keidanren.or.jp/policy/2020/079.html
(2) 柴田陽一，ほか：関数型暗号とブロックチェーンの組合せによる秘匿分散記録システムの試作，マルチメディア，分散協調とモバイルシンポジウム2018論文集，1879～1882 (2018)
(3) 一般社団法人 データ社会推進協議会：2020年度データ連携基盤技術報告書 スーパーシティのデータ連携基盤に関する調査業務 2021年３月第１版(2021)
https://data-society-alliance.org/survey-research/supercity_datamodel/

特集論文

システム連携を加速する大規模最適化問題の高速求解技術

柴田秀哉*
Hideya Shibata

Fast Algorithm for Large－Scale Optimization Problems Accelerating System Collaboration

要　旨

IoT(Internet of Things)技術の進展によって，様々な機器からのデータ収集が可能になると，それらのデータを活用した意思決定手段が重要になる。特に，複数のシステムが相互に連携して計画全体を最適化するSoS(System of Systems)では，最適化問題の規模が大きくなり，計画立案のための計算負荷が高いという課題がある。

この課題に対して，大規模最適化問題に対する高速求解技術を開発した。この手法の特徴は次の２点である。

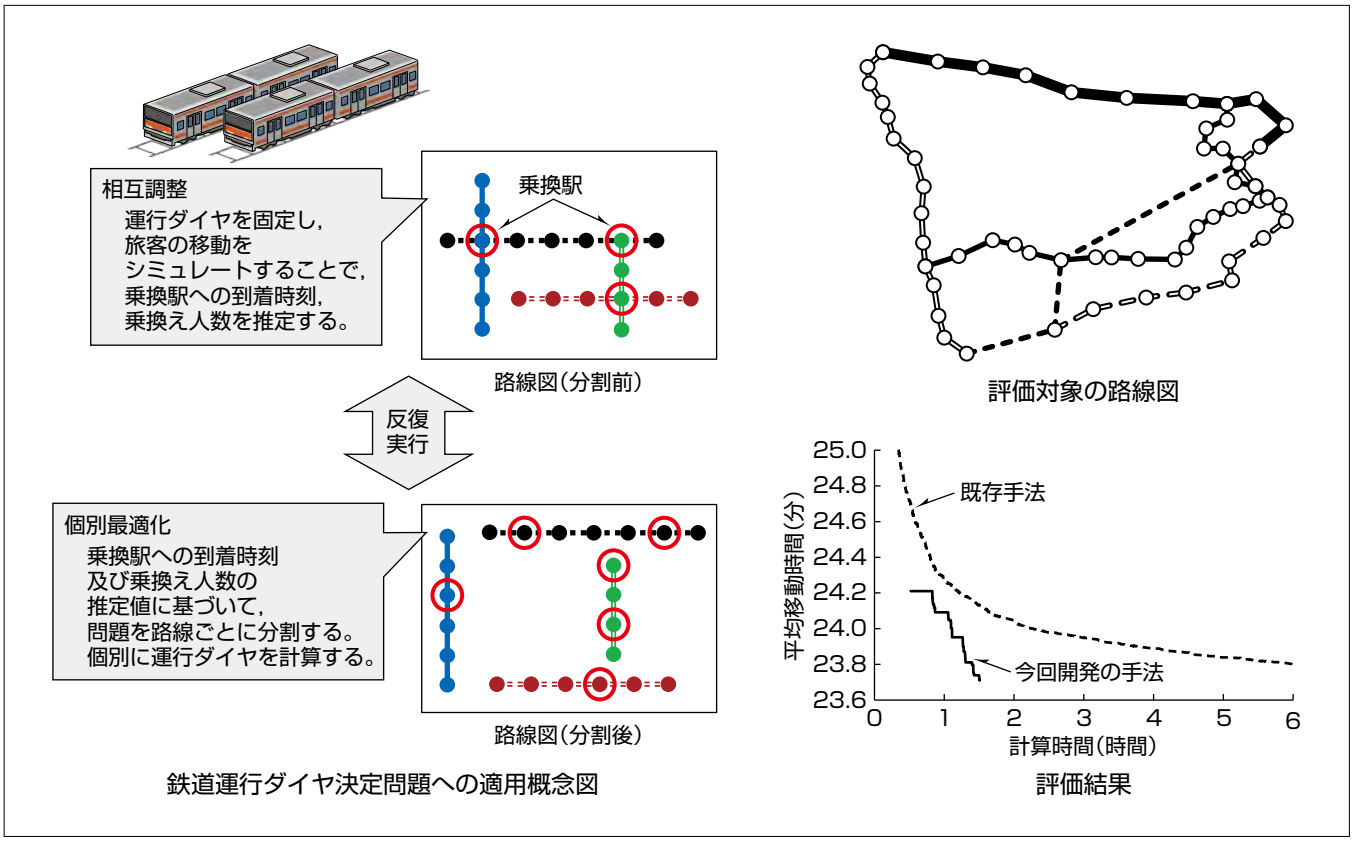
⑴　要素システム間の疎結合性に基づく問題分割

SoSを構成する個々の要素システムは，互いの入出力を介して緩やかに連携している。この疎結合性に基づいて，最適化問題を要素システムごとに分割する。

⑵　個別最適化と相互調整の反復的な実行

SoS全体の計画立案の問題を，要素システムごとの個別最適化と，要素システム間の相互調整との合成であると捉えて，両者の反復的な実行によって，高速かつ高精度な最適化計算を実現する。

この手法を複数の路線から成る鉄道の運行ダイヤ決定問題に適用し，評価を実施した。評価の結果，５路線の問題に対して，既存手法では計算時間が６時間を超えても到達できない精度の解を，この手法では計算時間90分で導出でき，その優位性を確認できた。



鉄道運行ダイヤ決定問題への適用概念図及び評価結果

鉄道運行ダイヤの決定をSoSの計画立案と見なす場合，各路線を要素システムと見ることができる。今回開発の手法では，路線ごとの運行ダイヤ決定(個別最適化)と，乗換えを伴う旅客の乗換え時刻を媒介とした相互調整との反復実行によって運行ダイヤを計算する。旅客の移動需要を既知とし，旅客の平均移動時間の低減を目的に，５路線90分間の運行ダイヤ作成について評価した結果，既存手法より短い計算時間で移動時間が短い解を導出できた。

*情報技術総合研究所

1. まえがき

IoT技術の進展によって，様々な機器データをリアルタイムに収集し，活用することが可能になりつつある。これに伴い，複数のシステムが相互に連携して意思決定を行うSoSの考え方が重要性を増してきている。

本稿では，SoSでの意思決定を支援する技術として，三菱電機が開発した大規模最適化問題の高速求解技術を述べる。SoSでの計画立案を大規模な最適化問題と捉えると，この問題は要素システムごとの個別最適化と，要素システム間の相互調整としてモデル化できる(**図1**)。この考え方に基づいて，今回開発の手法では，要素システムへの問題分割と反復的な相互調整によって，高速かつ高精度な最適化計算を実現する[1]。また，適用事例として，複数の路線から成る鉄道の運行ダイヤ決定問題の事例を述べる[2]。

2. 適用対象

今回開発の手法は，SoSの計画立案を対象としたものであり，SoSの特性である“要素システム間の疎結合性”及び“2種類の意思決定の併存性”という二つの性質を利用する。それに加えてこの手法では，計画立案にまつわる“時刻に基づく順序関係”に着目する。

この章では，これら三つの性質について，鉄道の運行ダイヤ決定問題を例に交えて述べる。

2.1 要素システム間の疎結合性

SoSを構成する個々の要素システムは，それ自体が一つの閉じたシステムであると同時に，他の要素システムと相互に関係性を持つ。前者は，要素システムがある程度の独立性を持つことを意味し，後者は，この独立性が完全ではないことを意味する。本稿では，このような状態を要素システム同士が疎に結合していると表現する。なお，要素システム間の相互関係は，ある要素システムからの出力が他の要素システムへの入力になることによって実現される。

鉄道の運行ダイヤ決定問題の例では，路線網をSoS，個々の路線を要素システムと見ることができる。個々の路線は，乗換駅という限定的な結合点によって，他の路線と関わりを持つ。この結合点がもたらす相互関係は，乗換えを伴う旅客の乗換駅への到着時刻という形で表れる。言い換えると，一方の路線からの旅客の到着時刻(出力)が，他方の路線での旅客の出発時刻(入力)になる。このように見ると，運行ダイヤ決定問題で，対象になる路線網は，要素システム間の疎結合性を持つことが分かる。

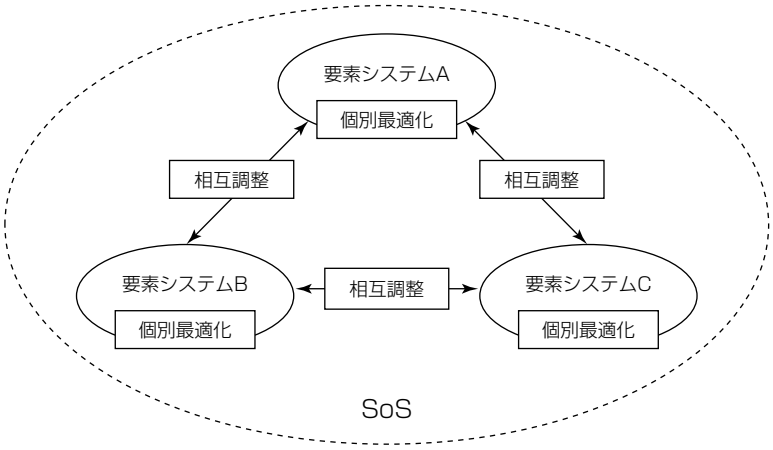


図1．SoSでの計画立案のモデル

2.2 2種類の意思決定の併存性

ここで言う2種類の意思決定とは，個別最適化と全体最適化である。SoSを構成する要素システムがある程度の独立性を持つと前提する以上，個別の要素システムは自身に閉じた目的と手段によって意思決定が可能であり，その志向を持つことは自然である。これが個別最適化の側面である。一方，他の要素システムとの関わりによって，双方が利益を得ることもまた珍しくはなく，この利益が個別最適化を志向するだけでは得られないこともまた明らかである。これが全体最適化の側面である。SoSの意思決定では，両方の側面が重要であり，どちらか一方を無視することは現実的ではない。

鉄道の運行ダイヤ決定問題の例では，単独の路線に関する情報だけを用いた個別の運行ダイヤ決定が個別最適化に該当する。列車運行の容易性や異常に対する頑健性などを優先すると，個別最適化による意思決定は最も簡単で確実である。しかしながら，乗換えを伴う旅客の満足度を考慮すると，他路線との関係性は無視できない。例えば，乗換駅での旅客の待ち時間を低減するには，個別最適化だけでは不十分であり，他路線との運行ダイヤの調整，すなわち全体最適化の観点が不可欠になる。

2.3 時刻に基づく順序関係

SoSに限らず，一般に計画立案やスケジューリングと呼ばれる問題では，決定対象のパラメータ間に，時刻に基づく順序関係が存在する。本稿で扱う鉄道の運行ダイヤ決定問題はスケジューリングの一種であり，この範疇(はんちゅう)に含まれる。

今回開発の手法では，時刻に基づく順序関係に着目し，計画立案の高速性と高精度性の両立を図る。その方法については，**3章**で述べる。

3. アルゴリズム

この章では，今回開発の手法のアルゴリズムについて，鉄道の運行ダイヤ決定問題を例に交えながら述べる。

3.1 基本方針

アルゴリズムは，三つの基本方針に基づいて設計される。これらの方針は，**2章**で述べた適用対象に関する三つの性質にそれぞれ対応する。

1点目は，要素システムごとへの問題の分割である。要素システム間の疎結合性を利用することで問題を分割し，一度に扱う問題の規模を低減させる。これによって，最適化計算の速度を向上させる。

2点目は，反復的な相互調整である。SoSが本質的には個別最適化と全体最適化という2種類の意思決定の併存であるという特性を利用し，要素システムごとの個別最適化と，要素システム間の相互調整を反復的に行う。ここでは，相互調整が全体最適化の手段になる。相互調整を行うことによって，問題分割による近似精度低下を抑制する。

3点目は，逐次的なパラメータの確定である。決定対象のパラメータ間に時刻に基づく順序関係が存在することを利用し，時刻が早い順にパラメータを逐次的に確定する。これによって，相互調整の反復回数を一定数以下に抑えて，計算速度を向上させる。

3.2 アルゴリズム

アルゴリズムの流れを**図2**に示す。次のとおり，図に従って各手順の詳細を述べる。

手順1では，各要素システムの初期状態，すなわち初期解を設定する。初期解の設定方法は適用事例に依存するが，基本方針としては，費用を度外視し，各要素システムを最大限稼働させるように設定する。システムの稼働という概念もまた適用事例に依存したものであるが，例えば，鉄道の運行ダイヤ決定では，ある時刻に列車を始発駅から出発させることを，その時刻でのシステムの“稼働”と見なすことができる。この場合，初期解としては，例えば毎分列車を走行させるような運行ダイヤが該当する。これは利用者から見ると理想的な状態であるが，費用面からは現実的ではない。

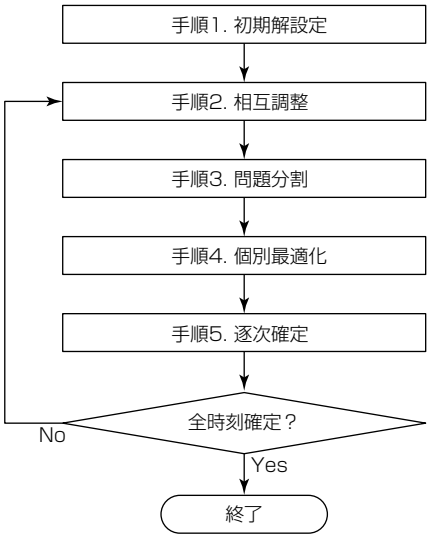


図2．アルゴリズムの流れ

手順2では，各要素システムの暫定状態に基づいて，要素システム間の相互調整を行う。数学的に表現すると，決定対象のパラメータ(変数)のうち，各要素システムに閉じたものを暫定解で固定した状態で，SoS全体に関する最適化問題を解く。これによって，各要素システム間でやり取りされる入出力が定まる。この入出力が相互調整の実体である。ここでは全体最適化の問題を扱うため，見かけ上の問題規模は大きくなるが，要素システムに閉じた変数を固定しているため，実際の問題規模は見かけほど大きくはない。

鉄道の運行ダイヤ決定の例で手順2で行うことは，旅客の乗換駅への到着時刻を計算することである。すなわち，個々の路線の運行ダイヤを固定した状態で，各旅客が目的地に最も効率良く移動するための移動経路，乗車すべき列車などを全体最適化問題によって計算する。これによって，乗換駅への到着時刻が得られる。乗換駅への到着時刻は，ある路線からの出力であると同時に，他の路線への入力でもある。

手順3では，手順2の相互調整の結果を受けて，問題を要素システムごとに分割する。他システムからの入力が手順2によって暫定的に与えられるため，各要素システムは，この暫定的な入力によって，自己の問題を独立した個別最適化問題と見なすことができる。鉄道の運行ダイヤ決定の例では，他路線から乗り換えてきた旅客の到着時刻に基づいて，各路線の個別の運行ダイヤ決定問題へと分割する。分割された問題では，他路線からの乗換え客と当該路線から移動を始める旅客は区別されない。

手順4では，手順3で分割された個々の問題を計算し，計算結果を暫定解として保持する。この手順は個別最適化に相当する。鉄道の運行ダイヤ決定の例では，各路線の運行ダイヤを個別に決定する。

手順5では，未確定のパラメータのうち，時刻の最も早いものを，手順4で計算した暫定解に基づいて確定させる。ここで確定させたパラメータは，後の反復で変更させることはない。全ての時刻に関するパラメータが確定されれば，アルゴリズムは終了する。未確定の時刻が存在する場合は，手順2に戻る。鉄道の運行ダイヤ決定の例では，最初の反復で最初の時刻，例えば6時0分のダイヤを確定する。す

なわち，６時０分の各駅での列車出発の有無を確定する。以降の反復で，６時１分，６時２分と逐次早い時刻についてのダイヤを確定させていく。

これらの各手順を，**3. 1節**で述べた三つの方針と対応付けると次のようになる。すなわち，要素システムごとへの問題の分割は手順３に，反復的な相互調整は手順２から手順５までの一連の処理の繰り返しに，逐次的なパラメータの確定は手順５にそれぞれ対応する。

4. 適 用 事 例

この章では，今回開発の手法を鉄道の運行ダイヤ決定問題に適用し，評価した結果について述べる。

4.1 評 価 条 件

評価は５路線57駅から成る路線網を対象とする(**図３**)。運行ダイヤ作成の対象期間は1.5時間(90分)とし，その期間内に移動する約21万の旅客を対象とする。運行ダイヤの良否は，旅客の平均移動時間で判定するものとする。

4.2 評 価 結 果

評価結果を**図４**に示す。図の縦軸は旅客の平均移動時間であり，横軸は運行ダイヤの計算時間を表す。実線が今回開発の手法，破線が比較用の既存手法にそれぞれ対応する。既存手法としては，最適化の分野で一般的に用いられる局所探索法を設定した[2]。今回開発の手法，既存手法共に反復解法であり，計算を継続すると解が改善されていくため，計算が進むにつれて，平均移動時間が短縮されていく。既存手法と比較して，今回開発の手法の解が階段状に改善されているのは，１回の反復に要する計算時間が大きく，かつ改善効果が大きいためである。

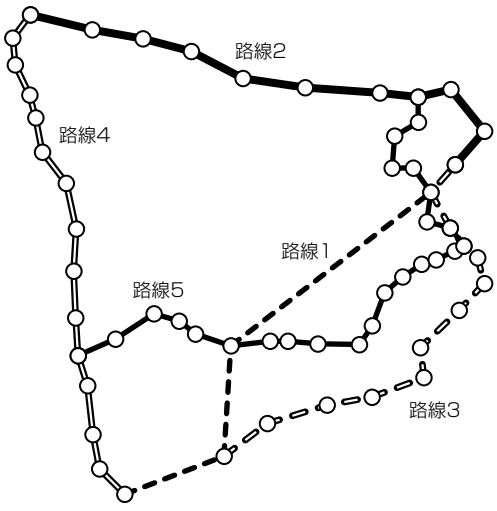


図３．評価対象の路線網

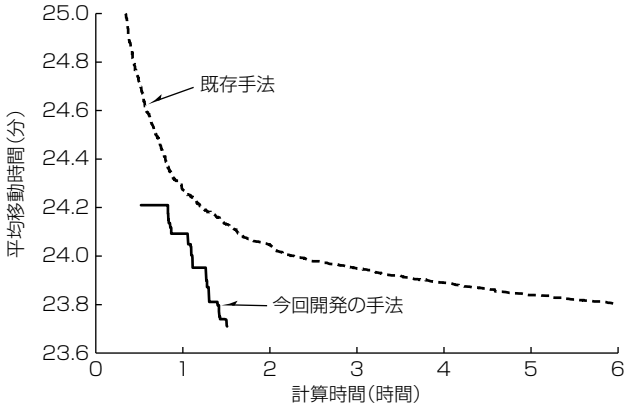


図４．評価結果

図４から，今回開発の手法は既存手法と比較して，精度の高い解を高速に導出していることが分かる。実際，今回開発の手法では計算時間が90分の時点で平均移動時間が23.7分の解を導出している。一方，既存手法では，計算時間が６時間を超えても同等の精度には至っていない。この結果から，５路線という規模の運行ダイヤ決定問題で，今回開発の手法の優位性が示された。

5. む す び

本稿では，SoSでの意思決定を支援する技術として，大規模最適化問題の高速求解技術を述べた。また，適用事例として，複数路線から成る鉄道の運行ダイヤ決定問題への評価結果を述べて，その優位性を示した。

本稿では述べきれなかったが，当社では，電力分野での発電機起動停止計画問題に対しても，今回開発の手法を適用する試みを行っている[3]。IoT技術の進展に伴い，今後，ますますSoSの意思決定は重要性を増していく。それに伴い，データに基づく定量的な計画立案手法が重要になる。今後は，この手法の適用対象を更に拡大し，システム連携を加速させていく。

参 考 文 献

(1) 柴田秀哉，ほか：複数系に跨るスケジューリング問題を対象とした部分問題分解に基づく最適化手法，日本オペレーションズ・リサーチ学会春季研究発表会アブストラクト集，30～31 (2020)
(2) 松永龍弥，ほか：移動需要に基づく鉄道運行計画決定問題に対する分解アルゴリズム，日本オペレーションズ・リサーチ学会和文論文誌，**64**，101～125 (2021)
(3) 松永龍弥，ほか：大規模な発電機起動停止計画問題に対する部分問題分解に基づく高速解法，電気学会全国大会講演論文集，6-076 (2021)

佐藤隆臣*
Takaomi Sato
川口嵩平*
Shuhei Kawaguchi
菊地健斗*
Kento Kikuchi

環境配慮型生産改善フレームワーク

Production Improvement Framework for Reducing Environmental Load while Maintaining Productivity

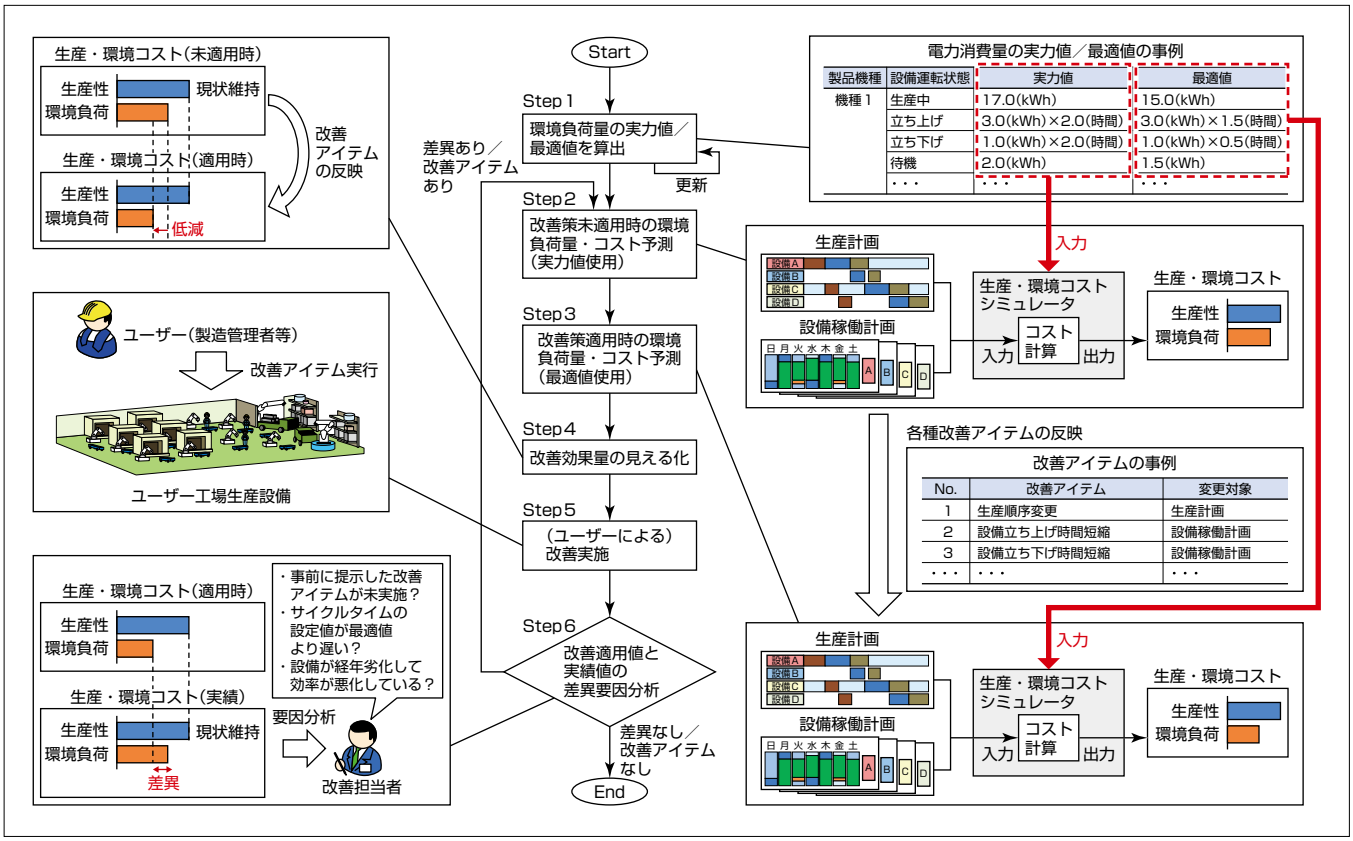
要　旨

持続可能な開発目標SDGs(Sustainable Development Goals)の一目標であるカーボンニュートラルの実現に向けた取組みを各国が推進している。特にエネルギー使用量や環境負荷排出量の多い製造業では無視できない状況で，現状の生産性を落とさずに環境負荷を低減することが課題になっている。

三菱電機グループでは，生産性と環境負荷を等価に扱い最適化する生産管理構想“Environment and Energy Just In Time[(1)]”を提唱し，この課題の解決を目指している。この構想の一環として検討している，シミュレーション技術を用いた，生産性と環境負荷との最適なバランスの決定を支援するフレームワークを提案する。このフレームワークでは，工場の生産設備における過去の電力，水，ガス等の資源の消費量と，有害物質の排出量の実績データから算出した実力値と最適値を用いて，今後予定されている生産での，改善策の適用有無による環境負荷排出量とコストの差異をシミュレーションすることで予測する。これらの差異を改善効果量として提示して，ユーザー中心に改善を実行してもらう。この改善サイクルの繰り返しで，最適な生産運用を実現する。

当社モータ製造工場の鉄心プレス設備で，このフレームワークを用いた改善に取り組んだ結果，生産性を維持しつつ，環境負荷量とコストを削減できた。さらに，２周目以降の改善で16%(42万円/年)の削減可能性を示した。

今後，このフレームワークを用いたソリューションの提供に向けて，当社工場での実証を重ねる計画である。



Environment and Energy Just In Time構想に基づく環境配慮型生産改善フレームワーク

まず，生産設備の過去の環境負荷量の実績データから実力値と最適値を算出する(Step１)。次に，今後予定されている生産での改善未適用時(Step２)と適用時(Step３)の環境負荷排出量とコストをシミュレーションで予測する。二つの予測値の差異を改善効果量として提示(Step４)し，ユーザー判断の下，改善実行してもらう(Step５)。最後に，適用時の環境負荷量／コストと実際の生産実績の差異要因を分析し，次回以降の改善アイテムを抽出する(Step６)。

1. ま え が き

2015年の国連サミットで採択された持続可能な開発目標SDGsの一目標であるカーボンニュートラル(CN)の実現に向けた取組みを各国が推進している[2]。代表的なものとして，中国の工業グリーン発展に関する第14次５カ年規画が挙げられる。

特にエネルギー使用量や環境負荷排出の多い製造業では，CNの実現は無視できない状況で，現状の生産性を落とすことなく環境負荷を低減することが課題になっている。

そこで，当社グループでは，生産性と環境負荷を等価に扱い最適化する生産管理構想“Environment and Energy Just In Time”を提唱し，この構想を用いた課題解決を目指している。

本稿では，シミュレーション技術を用いて，生産性と環境負荷との最適なバランスの決定を継続的に支援する，環境配慮型生産改善フレームワークを提案するとともに，当社工場での実証実験結果と今後の展望について述べる。

2. Environment and Energy Just In Time構想

Environment and Energy Just In Time構想は，原材料，労働力といった生産財と，電力や水といった環境負荷に関連する資源を必要な場所に，必要な量を，必要なときに投入し，生産性，環境負荷のバランスを取って全体最適化する構想である。従来の工場では，一般的に省エネルギーや環境負荷対策を生産と切り離して個別に対応し，生産に関係のない範囲での改善に終始していたため，今後厳しくなる環境法規制に対応する場合，生産に関係する範囲での改善も必要になることから，設備停止等で生産性の悪化を招くおそれがある(**図１**)。一方，Environment and Energy Just In Time構想では，環境負荷対策と生産を等価に扱い，環境負荷対策が生産(数量，時間等)に与える影響を定量化することで，環境法規制の制約下で，最大の生産性を上げる運用の実現を可能にする(生産性の悪化を最小限にとどめる)。等価に扱うとは，工場の生産，環境負荷を費用換算し，統一指標で評価することを意味する。

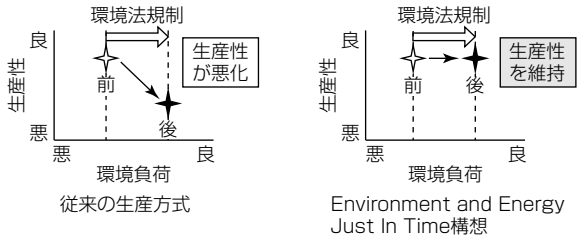


図１．Environment and Energy Just In Time構想に基づく生産管理イメージ

3. 環境配慮型生産改善フレームワーク

環境配慮型生産改善フレームワークでは，日々の生産に着手する前に，ユーザー(製造現場管理者等)に，環境法規制に対応しつつ，生産財や，環境負荷に関連する資源の消費や処理に応じたコストを最小化する生産運用計画と改善効果量を提示することで，ユーザーの改善実行を支援する。

このフレームワークの運用の効率化のため，過去の生産実績データから実力値と最適値を算出する機能と，それらの値をパラメータとして生産財や環境負荷に関連するコストを算出するシミュレーション機能を開発した。

3.1 実力値と最適値の算出

生産に伴い消費する電力，水，ガス等の資源量と，排出する温室効果ガス(CO_2)等の有害物質量の実力値と最適値の算出方法について述べる。今回は対象を電力消費量とする。

3.1.1 実力値の算出方法

電力消費量は，製品機種及び設備の運転状態(立ち上げ，生産中，立ち下げ，段取り替え等)に依存することから，実力値算出の準備として，電力消費量データに生産数量実績データを組み合わせて，データ集計を行う。製品機種及び設備の運転状態別に集計した電力消費量データから，**図２**に示すように，外れ値を除外した中央値を実力値とする。言い換えれば，“ユーザーが通常運用した”場合の設備の電力消費量のことである。なお，過去の経験から，データの分布が正規分布であることは稀有(けう)であることから，外れ値抽出方法として，四分位法(箱ひげ図)を用いた。

3.1.2 最適値の算出方法

実力値算出と同様の方法で，集計したデータの分布から，外れ値を除外した後の最小値を，最適値とした(**図２**)。“ユーザーがうまく運用すればここまでできる”場合の設備の電力消費量のことである。ここで，外れ値を除外する理由は，通常の生産とは別に試作品等でサイクルタイム(秒/個)を著しく落として生産したり，顧客からの特急オーダーで本来の設備スペックのサイクルタイムを超過して生産した

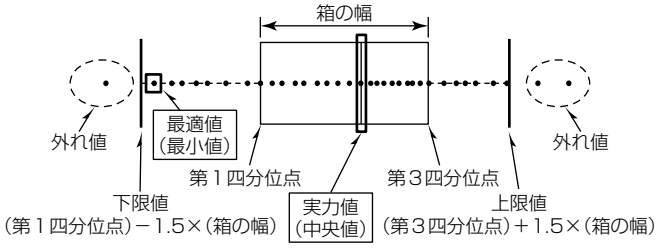


図２．四分位法(箱ひげ図)による実力値と最適値の算出方法

りすることがあるためである。

3.2　生産・環境コストシミュレータ

図3に生産・環境コストシミュレータの全体図を示す。このシミュレータは，以前から存在する生産財の使用量とコストを算出する生産コストシミュレータに，環境負荷量とそれに伴い発生するコストを算出する環境コストシミュレータを追加実装したものである[3]。

3.2.1　入出力データ

このシミュレータは，**表1**に示す生産システムパラメータ，環境負荷量／コストパラメータ，生産運用計画データの3種類のデータを入力して，各種生産財と環境負荷に関する量とコストを出力する。生産システムパラメータと環境負荷量／コストパラメータは，対象とする工場の設備の製造能力や構成等の静的な設計データである。一方，生産運用計画データは，シミュレーション実行時に都度変化する動的なデータである。これらの詳細な設定データを持つことで，実際の設備の挙動を再現することが可能になる。**3. 1節**で算出した実力値と最適値は，この生産システムパラメータ，環境負荷量／コストパラメータとして用いる。

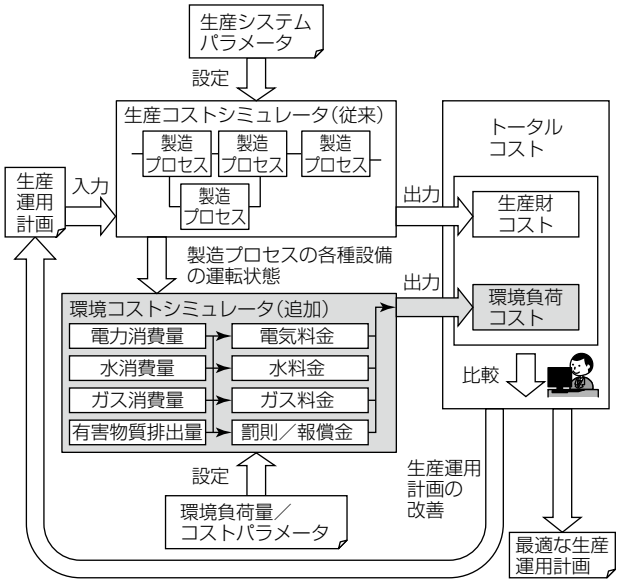


図3．生産・環境コストシミュレータ

表1．生産・環境コストシミュレータ入力データ

生産システム パラメータ	環境負荷量／ コストパラメータ	生産運用計画 データ
・生産設備構成(製造プロセスのつながり) ・製造能力(サイクルタイム，リードタイム等) ・製品機種 ・(製品1個当たりの)材料使用量 ・労働力(作業員人数) ・段取り替え時間 ・作業シフト(時間) ・稼働日カレンダー ・生産財の単価	・各種生産設備の運転状態ごとの環境負荷量 ・電気・水・ガス等の料金表 ・環境法規制に伴う罰金／報償金	・生産計画 ・設備稼働計画

3.2.2　使 用 方 法

各種改善アイテムに応じて，生産システムパラメータ，環境負荷量／コストパラメータ，生産運用計画データを変更し，それに応じたコストを算出することで，改善アイテムの効果を確認する。改善担当者やユーザーが，改善効果が最大になるように，各種データの変更を繰り返して使用することを想定している。

ただし，効果が最大になるデータを探索する作業は工数がかかるため，現在，生産計画の一部を対象に自動化を進めている。

3.3　フレームワーク実施手順

今回提案する環境配慮型生産改善フレームワークでは，次に示すStep 1 ～ 6 の手順を繰り返し実行することを想定している。

⑴　Step 1 ：実力値と最適値を算出

生産設備の過去の電力，水，ガス等の資源の消費量と，温室効果ガス等の有害物質の排出量の実績データの分布から，実力値と最適値を算出する。

⑵　Step 2 ：改善策未適用時の環境負荷量・コスト予測

改善担当者が，通常運用した場合，すなわち改善策未適用時の生産財及び環境負荷に関する量とコストを算出する(以下“未適用値”という。)ため，実力値を入力して，シミュレーションを実行する。

⑶　Step 3 ：改善策適用時の環境負荷量・コスト予測

改善担当者が，設備立ち上げ／立ち下げ時間の短縮や，段取り替えの組合せの変更等の様々な改善アイテムを，生産運用計画やパラメータに反映し，生産財及び環境負荷に関する量とコストをシミュレーション(最適値使用)によって算出する(以下“適用値”という。)。

⑷　Step 4 ：改善効果量の見える化

各種改善アイテムを適用して，Step 2 の改善未適用値から，Step 3 の適用値に近付けることを目的に，未適用値と適用値の差分を，改善効果量として出力し可視化する。

⑸　Step 5 ：(ユーザーによる)改善実施

改善効果量をユーザーに提示し，了承を得た上で，ユーザー中心に改善実行してもらう。

⑹　Step 6 ：改善適用値と実績の差異分析

改善担当者が，生産時に実績値を収集し，改善適用値との差異要因を分析し，次回以降の改善アイテムを抽出する。

4. 実 証 実 験

当社モータ製造工場の鉄心プレス設備で，環境配慮型生産改善フレームワークを用いて，“現状の生産性を落とすこ

となく，環境負荷を低減することが可能であるか”という仮説を実証するための実験を行った。

4.1 実 験 条 件

⑴ 対象生産設備

工場の中で，環境負荷に関する資源消費量(今回の場合，電力消費)の多いモータ鉄心プレス設備を含む３生産ライン

⑵ 対象期間

2022年１月31日～２月11日(約２週間)

⑶ 実力値／最適値算出に用いたデータの対象期間

2020年４月１日～2021年３月31日(１年間)

⑷ 対象とする生産財と環境負荷資源

①生産財：労働力(労務費)

②環境負荷資源：電力(電力料金)，CO_2(排出量取引費用)

なお，CO_2排出量は電力消費量から換算し，CO_2に関するコストは中国の一部の省で用いられているCO_2排出量取引費用を用いた(取引レート：約1,000円/t－CO_2)。

⑸ 改善アイテム

製品品質や納期等生産性を悪化させないことを制約とした場合，今回実施可能な改善アイテムは次の三つであった。

①改善アイテム１：生産順序変更

②改善アイテム２：(生産開始前の)設備立ち上げ時間の短縮

③改善アイテム３：(生産終了後の)設備立ち下げ時間の短縮

4.2 実験結果・考察

フレームワークのStep１実施によって，製品機種Aを生産する際の設備の運転状態別(立ち上げ，立ち下げ，段取り替え，生産中)の電力消費量の実力値と最適値を算出した例を**表２**に示す。**表２**に示した結果も含む全製品機種の設備運転状態別の実力値と最適値を用いて，フレームワークを１周(Step１～６)させた際の，生産財及び環境負荷に関する改善未適用値，適用値，実績値の３種類のコスト(年間換算)を**表３**に示す。今回の実験では，主に改善アイテム３実施による効果で，生産性を落とさずに(今回のケースでは2.3％向上)，環境負荷量とコストを1.5％低減できた。なお，過去の評価で，今回の実験とは別の期間のデータを用いて，シミュレーションで算出した未適用値と，改善未実施の場合の実績値の差異が十分に小さいこと，つまり，今回提示する改善効果量を見誤るほどの差異がないことを確認している。

一方で，環境負荷コストに関する(改善)適用値と実績値の間には，14％の差異があったことから，ユーザーへのヒアリングやデータの確認で要因分析した。結果，**表４**に示す問題点が明らかになった。それに加えて，これらの問題を解決するために，２周目以降の改善アイテムを抽出し効果量を算出したところ，１周目と合わせて42万円/年の環境負荷コストを削減可能であることが分かった(**表４**)。

表２．電力消費量の実力値と最適値の算出例

製品機種	設備運転状態	実力値	最適値
機種A	立ち上げ	5.1(kWh)(３時間)	1.0(kWh)(１時間)
	立ち下げ	3.2(kWh)(２時間)	1.0(kWh)(１時間)
	生産中	2.3×10^{-3}(kWh/個)	2.0×10^{-3}(kWh/個)
機種A→機種B	段取り替え	2.0(kWh)(２時間)	1.0(kWh)(１時間)

表３．改善１周目の生産財と環境負荷コスト

	生産財	環境負荷	
	労務費(万円/年)	電力(万円/年)	CO_2(万円/年)
未適用値	555	322	18
適用値	453	272	15
実績値	542	318	17

表４．２周目以降の改善アイテムと効果

問題点	改善アイテム	電力(万円/年)	CO_2(万円/年)
生産中のサイクルタイム設定値が設備スペックに比べて低い	サイクルタイム設定値を設備スペックの最小値で運用する	25.2	1.4
設備故障(コントローラ基板)を懸念して，生産終了後に設備立ち下げ未実施	制御盤内熱環境の向上(熱交換器の増設／更新)	8.0	0.4
	問題箇所の分離(制御盤内の電源回路の分割)		
生産中の１回当たりの材料交換作業時間が長い	作業標準化(熟練者の取組みを初級者に教育)	1.8	0.1
	作業環境の向上(ヘッドライト等の照明の有効活用)		
	(材料挿入専用の)治具の改良		

今回の実証実験によって，生産性を落とさずに，環境負荷量とコストを低減することが可能であることを示したが，一方で，環境法規制を考慮した生産改善の実施までには至らなかった。

5. む す び

本稿では，生産性と環境負荷との最適なバランスの決定を支援する環境配慮型生産改善フレームワークを提案した。

実証実験の結果，フレームワークを用いた１周目の改善によって，生産性を落とすことなく，環境負荷を1.5％低減することが可能であることを示した。それに加えて，２周目以降の改善で42万円分/年の環境負荷量とコストを削減可能であることを示した。

今後は，このフレームワークを用いたソリューション提供を目指して，当社工場での実証実験を重ねる。

参 考 文 献

⑴ 三菱電機㈱：三菱電機の経営戦略，2021年度 経営戦略説明会【2021年６月３日】，20 (2021)

⑵ 経済産業省 資源エネルギー庁：エネルギーに関する年次報告(エネルギー白書2021)，29～52 (2021)

⑶ 生産性と環境負荷の最適バランス決定を支援するシミュレータ，三菱電機技報，**95**，No.1，34 (2021)

特集論文

省人化・非対面ソリューションを実現する多用途移動ロボットシステム

Versatile Mobile Robot System Realizing Contactless and Manpower Saving Solutions

赤穂賢吾*
Kengo Akaho
銭谷　享†
Susumu Zeniya
宮岡俊輔†
Shunsuke Miyaoka

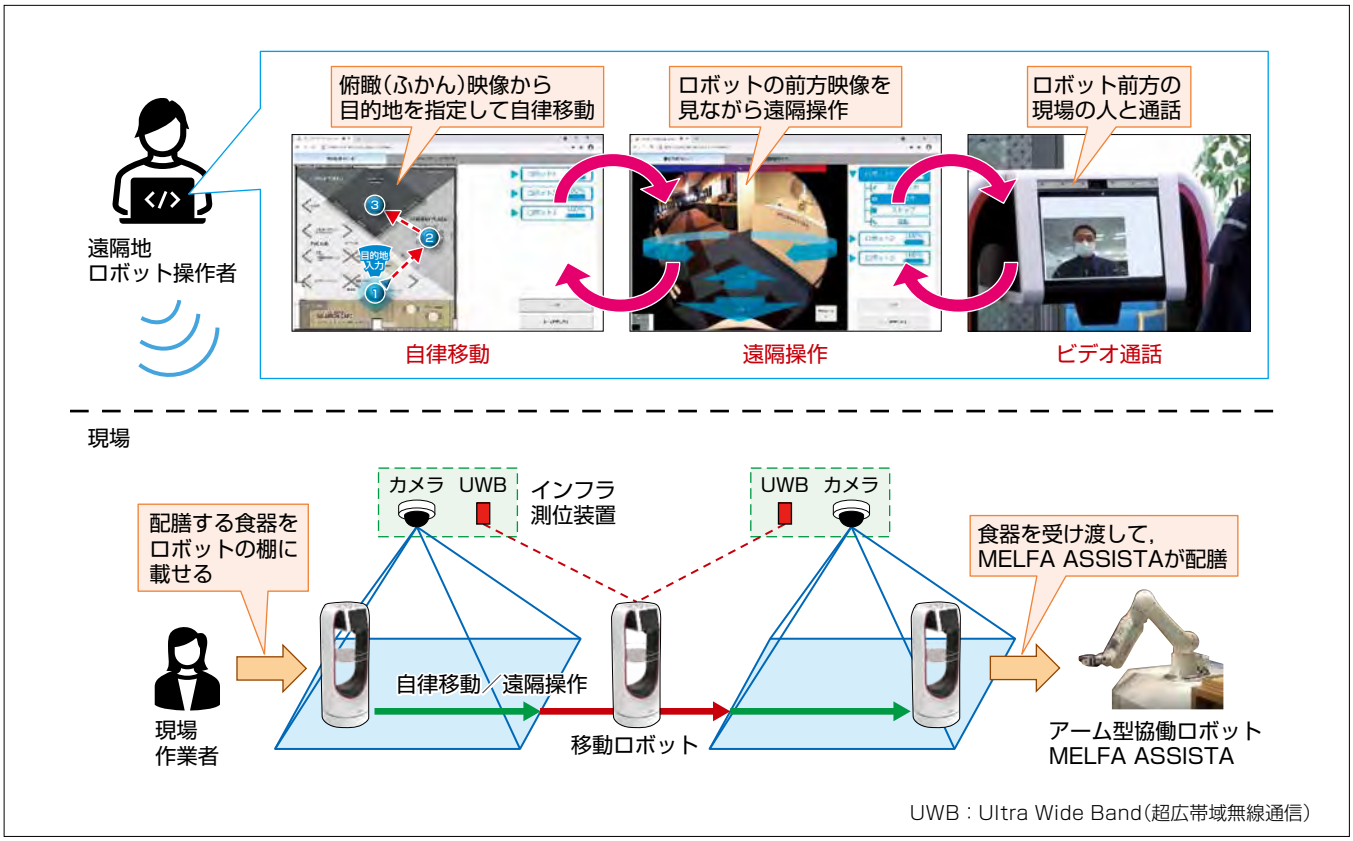
要　旨

人手不足，少子高齢化の社会課題に対して求められているDigital Transformation（DX：進化したデジタル技術を浸透させることで人々の生活をより良いものへと変革する）を，多用途移動ロボットの活用で実現することを目指している。

このロボットは，自律的に作業を行いつつ状況次第で人が介入して遠隔操作することで，定型作業だけでなく非定型作業への対応を可能にする。ユースケースの例として，ホテル業務の省人化を実現する“業務ピークを考慮したホテル業務支援”，時間的・空間的制約にとらわれない“対面を実現するロボット操作遠隔勤務”を想定している。

今回，Proof of Concept（PoC）設計・構築・評価，顧客からのフィードバックによる検証のサイクルを繰り返して，顧客受容性と技術的実現性を高める第1段階として，ユースケースを限定した実証を実施した。今回の実証では三菱電機製アーム型協働ロボットMELFA ASSISTA[(1)]と協調した食器配膳と，ビデオ通話を活用した遠隔地コミュニケーションの役割を兼ねる多用途移動ロボットシステムを開発した。この多用途移動ロボットシステムはDX，スマートシティをテーマとした三菱電機のソリューションを展示する場である“XCenter（クロスセンター）[(2)]”に展示し，顧客からのヒアリングを実施中である。

今後は得られた知見を生かして，PoCのサイクルを繰り返すことで顧客受容性の高いソリューションを実現する。



ユースケース：アーム型協働ロボットMELFA ASSISTAと協調した食器配膳

多用途移動ロボットシステムと当社製アーム型協働ロボットMELFA ASSISTAが協調した食器配膳とビデオ通話を活用した遠隔地コミュニケーションを実現する。遠隔地ロボット操作者はタブレット等の遠隔操作端末を用いて自律走行／遠隔操作／ビデオ通話を切り替えつつロボットを操作する。

*先端技術総合研究所　†ビジネスイノベーション統括事業部

1. まえがき

近年，DXの推進に伴って，サービスロボットの市場が拡大している。特に，少子化社会で働き手が不足していく中，持続可能な社会実現に向けて，人手不足の解消及びエッセンシャルワーカーの負荷低減としてのロボットの需要が拡大している。また，新型コロナウイルス感染症(COVID-19)の影響で非対面を実現する移動型テレプレゼンスロボットの需要も高まっている。

そこで，省人化・非対面ソリューションの実現に向けて，テレプレゼンス機能を持つ多用途移動ロボットシステムの開発を進めている。

2. コンセプト

これまでのロボットは工場内搬送を行う自律型移動ロボット等，定型作業を行うロボットが主流であった，しかし，省人化・非対面ソリューションを実現するには定型作業の遂行だけではなく，非常時の対応も含めて，人間のように状況に応じた対応を行うことが重要である。

そこで，当社はテレプレゼンス機能を持った多用途移動ロボットの実現を目指している。このロボットでは，自律的に定型作業を遂行しつつ，状況次第で人が介入して遠隔操作(テレプレゼンス)を行い，非定型作業を行うことで多用途に活用可能にする。ユースケースの例として，ホテル業務の省人化を実現する“業務ピークを考慮したホテル業務支援ユースケース”や，“時間的・空間的制約にとらわれず対面と同等な非対面作業を実現するロボット操作遠隔勤務ユースケース”を想定している。

この章ではこれらについて述べる。

2.1 ホテル業務支援ユースケース

ホテルでは従業員１人に対して多種多様な業務が存在し，時間帯・状況に応じてピークになる業務が異なるため，従業員はピークに応じて動的に作業を切り替えている。そのため，ロボット等によって，一つの定型作業の効率化を図ったとしても十分な省人化は実現できないと考えられる。そこで，時間帯・状況に応じてロボットが次のとおり振る舞うことで従業員の業務を支援する。

(1) 宿泊客チェックイン時間に宿泊客の手荷物を客室に搬送する。
(2) 朝食／夕食時間帯に宿泊客をレストランに誘導する。
(3) レストランでテーブル-キッチン間を移動し，食器を運ぶことで配膳・片付けを支援する。
(4) 夜間に施設を巡回し，倒れている人／ゴミ／忘れ物を見つけたときにホテル担当者へ緊急連絡を行う。
(5) 夜間に客室清掃に使用するアメニティやシーツ等を各フロアのリネン室に配送する。
(6) 迷子／忘れ物発生時に該当箇所を探索し，探索結果をホテル担当者へ連絡する。
(7) 災害発生時に分岐箇所に移動し，適切なルートでの避難を案内する。

これによって状況に応じた業務ピークの効率化を図ることが可能になり，省人化に貢献できると考えられる。

2.2 ロボット操作遠隔勤務ユースケース

現在，メールや通話を駆使して，空間的制約を受けることなく業務を担当できるリモートワークが浸透しつつある。一方，リモートワークが難しい現地作業が存在することも多く，会社への出社が必要になるケースもある。空間的制約・身体的制約等で出社が難しい状況では業務内容が限定されてしまう課題がある。

そこで，リモートワーク中に必要に応じて自身の分身になるロボットを自宅から遠隔操作することで次のような非対面の遠隔業務を実現する。

(1) 来訪者受入れ時に遠隔地から担当者がビデオ通話で作業場所に案内する。そのまま協調して作業実施する。
(2) 建屋内の機器に異常が発生した際に，機器の近くまで移動し，カメラで遠隔確認する。
(3) ロボットを介することで身振り手振り等のノンバーバルコミュニケーションを補完し，対話しやすい状況を作り出す。

これによって空間的制約・身体的制約で出社できない人が担当可能な業務の幅を広げることが可能になり，人手不足の解消に向けた雇用創出を実現する。

3. PoCによる実現可能性検証

２章で述べたコンセプトを実現する多用途移動ロボットシステムの開発に当たって，事業化／拡大の確度を向上させるには顧客受容性と技術的実現性を高める必要がある。顧客受容性を高めるには顧客が既に認識している顕在ニーズだけではなく顧客がまだ気付いていない潜在ニーズも重要である。そのため，PoC設計・構築・評価，顧客からのフィードバックによる検証のサイクルを繰り返して，潜在ニーズの明確化を進める。

今回，PoCの第１弾としてホテル業務支援のユースケースの一つである食器配膳を当社製アーム型協働ロボットMELFA ASSISTA[1]と協調して行う多用途移動ロボットシステムを開発した。このPoCでは技術的実現性の検証，動く物を題材とした顧客との対話による顧客要求掘り出し

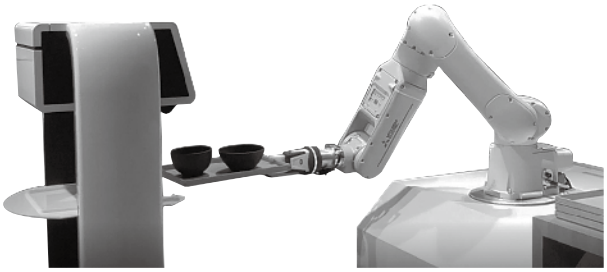


図１．多用途移動ロボットとMELFA ASSISTAの協調

を目的とする。

PoCのシナリオを次に示す。

⑴ 遠隔操作者の配膳開始の指示に応じて，多用途移動ロボット(以下“ロボット”という。)はホームポジションから食器受取位置に移動する。

⑵ 現場作業者がロボットに設置された棚に食器が載ったトレイを置く。

⑶ 食器を並べるMELFA ASSISTAへの受渡し位置に移動する。トレイを受け渡した後，ロボットはホームポジションへ帰還する。トレイ受渡しの様子を**図１**に示す。

なお，現場作業者から遠隔操作者にロボットが食器の配送を開始した旨を伝えるなど，コミュニケーションする必要がある際は，ロボットを介して遠隔操作者と現場作業者のビデオ通話を行うことが可能である。

実証の結果，このシナリオで，次の機能が技術的に実現可能であることが確認できた。多用途移動ロボットシステムが備える機能の詳細は**４章**に示す。

①遠隔から指定した箇所に自律移動できること。

②遠隔からロボット前方を撮影したカメラの映像を確認しながらロボットの移動を操作できること。

③ビデオ通話によって，遠隔操作者と食器配膳者がコミュニケーションできること。

④自律移動／遠隔操作／ビデオ通話をシームレスに切替え操作可能であること。

この多用途移動ロボットシステムはDX，スマートシティをテーマとしたソリューションを展示する場であるXCenterに展示し，顧客からのヒアリングを実施中である。

さらに，PoC第１弾の知見を収集しつつ，ホテルでのフロア間移動手荷物搬送業務等を行う社外実証を顧客とともに検討中である。フロア間移動はVille-feuille[(3)]を活用したエレベーター連携での実現を想定している。

4．多用途移動ロボットシステムの詳細

この章では今回のPoCで開発した多用途移動ロボットシステムの詳細について述べる。

4.1 システム構成

多用途移動ロボットシステムは天井カメラ，UWBを搭載するインフラ測位装置，ロボット，ロボット操作者が持つ遠隔操作端末，これらを統括するサーバ部で構成され，5G(第５世代移動通信システム)／LTE(Long Term Evolution)／Wi-Fi[(注1)]で相互通信する。システム構成図を**図２**に示す。サーバ部は，カメラ処理，センサ処理，俯瞰映像作成処理，モビリティ管制処理とロボット操作を実現するアプリケーションを含んで，今回はオンプレミスで構成した。このサーバ部は一部又は全てをクラウドサーバに構築することもできる。

ロボットは天井カメラ，UWBのインフラ測位装置が設置されている領域では，あらかじめ構築した地図情報が存在しない場合やレイアウトが頻繁に変更になるエリアでも自律走行を行うことが可能になる。

(注１) Wi-Fiは，Wi-Fi Allianceの登録商標である。

4.2 備える機能

多用途移動ロボットシステムは遠隔操作機能・自律走行機能・遠隔ビデオ通話機能を持ち，これらは遠隔操作端末で実行可能である。

4.2.1 自律走行

自律走行では遠隔操作者が俯瞰映像上でロボットの経由地，目的地を設定することで，ロボットが走行経路を設定し，移動を行う。移動経路上に障害物が存在するときは回避経路を生成し，障害物を回避して走行する。自律走行の操作画面を**図３**に示す。

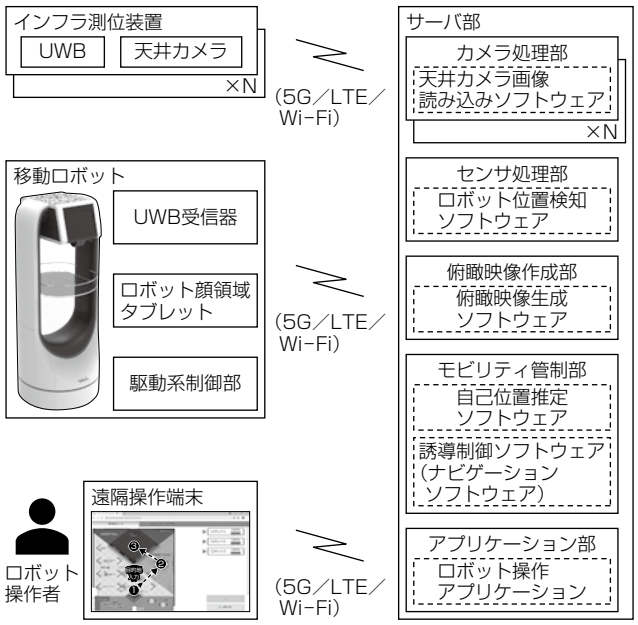


図２．システム構成

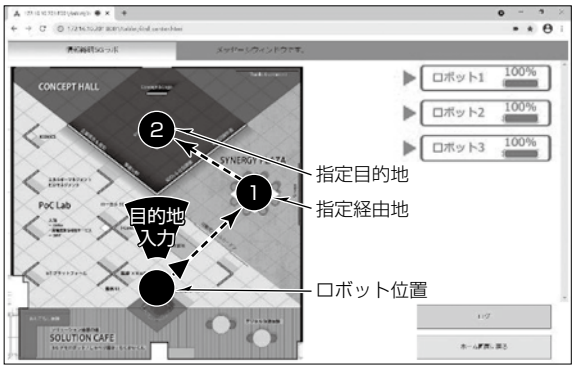


図３．自律走行の操作画面

図６．遠隔ビデオ通話の様子

4.2.2 遠隔操作

遠隔操作はロボットの前方を撮影しているカメラ映像を見ながら，二つの移動操作モードを必要に応じて切り替えて操作する。

一つ目の移動操作モードであるClicktoDriveは遠隔操作端末上で移動したい箇所をタッチすることでロボットの移動先を指定するものであり，遠方に移動する際に効果的である。**図４**にClicktoDriveの操作画面を示す。十字の領域がLiDAR(Light Detection And Ranging，光を用いて対象までの距離を計測する装置)の情報を基にした走行可能領域であり，領域内をタッチするとマーカが表示された上で，ロボットがマーカ地点まで移動する。

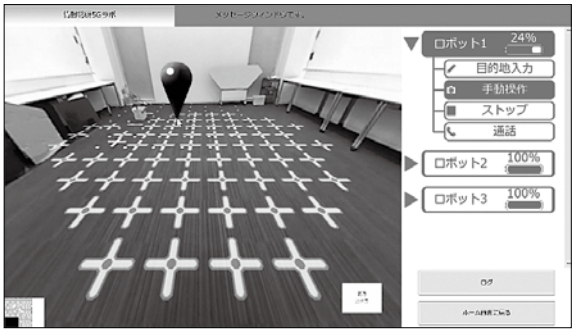


図４．ClicktoDriveの操作画面

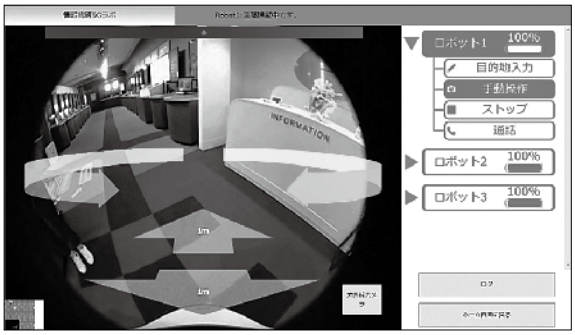


図５．DirectDriveの操作画面

二つ目の移動操作モードであるDirectDriveは移動量と移動方向又は回転方向を指定して移動するものであり，細かく位置を調整したい際に効果的である。**図５**にDirectDriveの操作画面を示す。前進，後進を指示する前後矢印や回転を指示する回転矢印をタッチするとロボットが移動する。

4.2.3 遠隔ビデオ通話

遠隔ビデオ通話は遠隔操作端末とロボット間で映像付きの通話を可能にする。ロボット側は顔領域に設置されたタブレットに遠隔操作端末のカメラ映像が表示され，遠隔操作端末側ではロボットの顔領域に設置されたカメラの映像が表示される。遠隔ビデオ通話の様子を**図６**に示す。

通話は遠隔操作者側，ロボット側のどちらからも発信可能であり，遠隔操作者からの現場に対する声掛けや，現場にいる人から遠隔操作者への問合せに活用可能である。

5. むすび

本稿では，省人化・非対面ソリューションを実現する多用途移動ロボットシステム実現に向けた取組みとともに，第１弾のPoCとして開発した食器配膳と遠隔地コミュニケーションのユースケースを実現する多用途移動ロボットシステムについて述べた。

現在，第１弾PoCの実証，検証中であり，今後は得られた知見を生かしたPoC設計・構築・評価を行い，検証のサイクルを繰り返す。これによって顧客受容性の高いソリューションを実現し，当社のロボット事業拡大につなげる。

参考文献

(1) 三菱電機㈱：協働ロボットMELFA ASSISTA製品特長
https://www.MitsubishiElectric.co.jp/fa/products/rbt/robot/pmerit/assista/index.html
(2) 三菱電機㈱：三菱電機が目指すDX・スマートシティを体感する場所，XCenter(クロスセンター)
https://www.MitsubishiElectric.co.jp/business-innovation/xcenter/
(3) 三菱電機㈱：スマートシティ・ビルIoTプラットフォームVille-feuille
https://www.MitsubishiElectric.co.jp/smartbuilding/ville-feuille/

特集論文

耐量子計算機暗号 ―量子コンピュータによる解読にも耐え得る次世代暗号―

川合　豊*
Yutaka Kawai
廣政　良†
Ryo Hiromasa
相川勇輔‡
Yusuke Aikawa

Post－Quantum Cryptography
―Next Generation Encryption Technology Resistant to Quantum Computing―

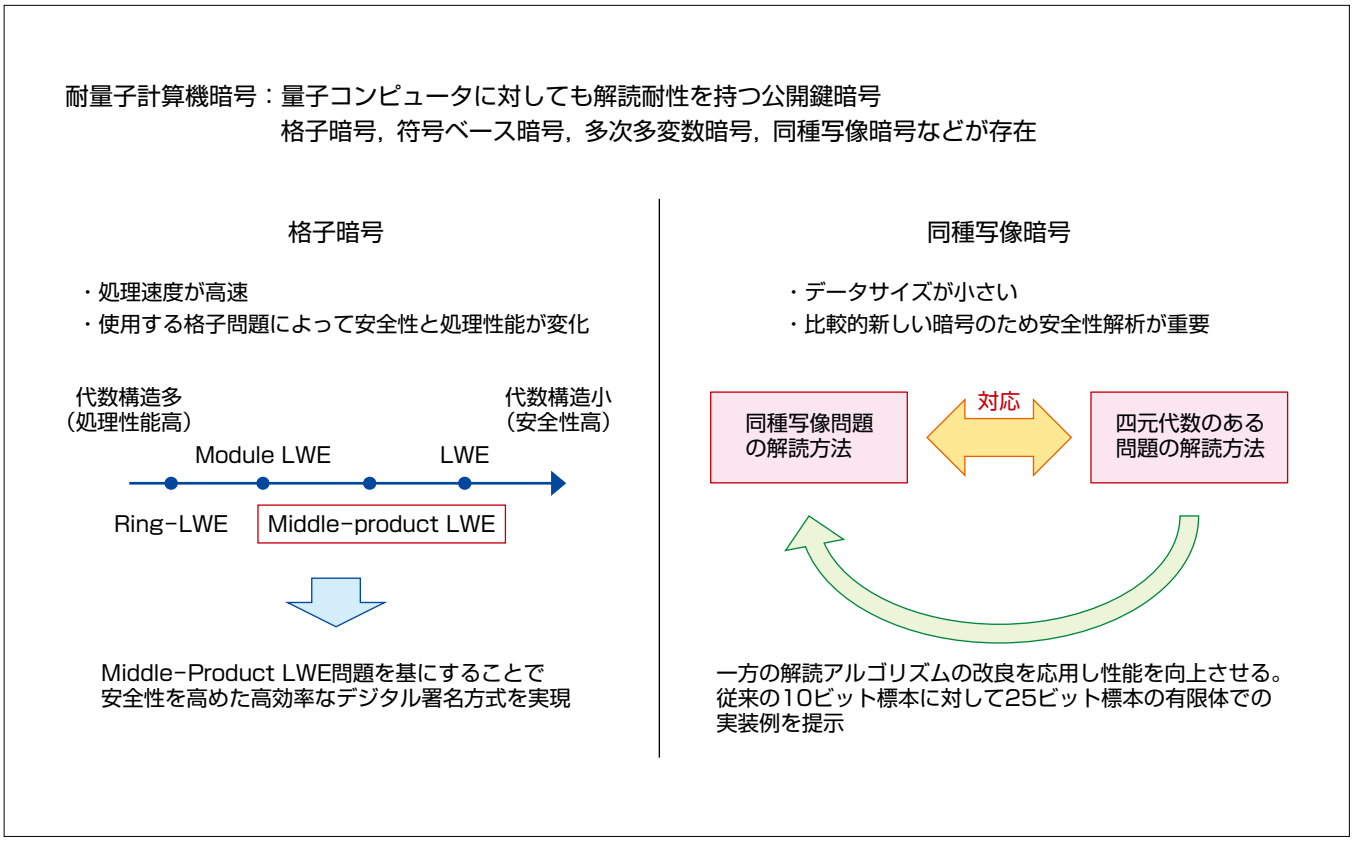
要　旨

将来，大規模な量子コンピュータが実現された場合，現在インターネットなどで広く使用されているRSA（Rivest Shamir Adleman）暗号や楕円（だえん）曲線暗号などの公開鍵暗号が解読されてしまうことが分かっている。そこで，そのような量子コンピュータが登場しても解読されないことが期待される公開鍵暗号“耐量子計算機暗号”の研究が盛んに行われている。

耐量子計算機暗号の研究は米国標準技術研究所（National Institute of Standards and Technology：NIST）の標準化計画を中心に様々な研究が進んでいる。耐量子計算機暗号は安全性を保証するために利用する数学的問題の違いから様々な種類の暗号がある。

これらの背景の下，処理速度が高速な“格子暗号”と，鍵のデータ長などが小さい“同種写像暗号”に着目し研究を進めている。これまでに格子暗号では，公開鍵暗号の一つの用途であるデジタル署名方式について，高安全化を実現した。同種写像暗号は格子暗号と比べて安全性解析の研究途上の暗号である。そこで安全性や効率性に関して，理論と実装の両面から解析を進めて，同種写像暗号の安全性や効率に関する知見を得た。

NISTの標準化選定が途中段階であることなどからも分かるように，耐量子計算機暗号はまだまだ研究途上の分野であり，研究動向の注視と，解析・設計技術の向上が必要不可欠である。そこで，今後も高安全かつ高効率な耐量子計算機暗号の実現を行い，安心・安全な社会の実現に貢献していく。



耐量子計算機暗号の種類と格子暗号・同種写像暗号の安全性解析の結果

量子コンピュータに解読耐性を持つと期待される耐量子計算機暗号のうち，処理速度が高速という特長を持つ格子暗号と，データサイズが小さいという特長を持つ同種写像暗号に関して効率化や安全性解析を行った。格子暗号に関しては比較的新しいMiddle-product LWE（Learning With Errors）問題を基にしたデジタル署名を実現し，同種写像暗号では他の代数（四元代数）の問題に置き換えて解析を実施し従来より長いビット長に対する攻撃を成功させた。

*情報技術総合研究所（博士（科学））　†同研究所（博士（情報学））
‡同研究所（博士（理学））

1. まえがき

現在，個人情報などの重要な情報がインターネット上などでやり取りされる際，それらを守るために様々な暗号技術が使用されている。中でも公開鍵暗号は，データの秘匿だけでなく，通信相手が正規のユーザーであるかを検証する相手認証などに広く利用されている。現在広く使用されている公開鍵暗号として，RSA暗号や楕円曲線暗号がある。RSA暗号は素因数分解問題，楕円曲線暗号は楕円離散対数問題が利用されており，これらの問題が現在のコンピュータでは現実的な時間で解読不可能であることから安全性の保証になっている。しかし，これらの問題は大規模な量子コンピュータが実現された場合，Shorのアルゴリズムによって現実的な時間で解読されてしまうことが知られている。

そこで，量子コンピュータに対しても解読耐性を持つことが期待される耐量子計算機暗号の研究が盛んである。耐量子計算機暗号の研究はNISTが主導する標準化選定を中心に動いている[1]。NISTでは2017年11月まで標準化候補の方式募集を行った。その後２回の選定が行われ，現在第３回の選考（第３ラウンド）中である[注1]。締切り時点では82方式の投稿があったが，第３ラウンドでは最終候補７候補と次点候補８候補まで選定されている。第３回の選考は2023年頃までに終了すると言われており，2024年頃には耐量子計算機暗号の標準規格を選定する計画になっている（**図１**）。

耐量子計算機暗号は，格子暗号，符号ベース暗号，多次多変数暗号，同種写像暗号などの種類が存在する。このうち，本稿では，処理が高速な格子暗号，データサイズが小さい同種写像について述べる（**表１**）。

（注１） 2022年５月現在。７月に第３ラウンドが終了し，CRYSTALS-KYBER，CRYSTALS-DILITHIUM，FALCON，SPHINCS+の標準化が決定した。

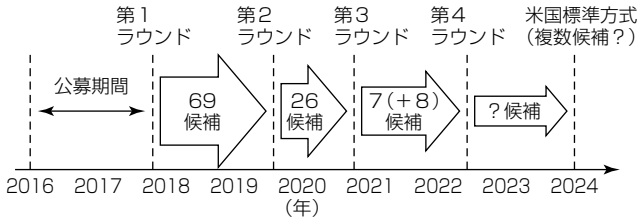


図１．NIST標準化の流れ

表１．格子暗号と同種写像暗号の比較

	格子暗号	同種写像暗号
鍵サイズ	従来の楕円曲線暗号と比較して10倍以上	従来の楕円曲線暗号と同程度
処理速度	高速	低速
NIST標準化候補	最終候補に５方式が選定（CRYSTALS-KYBER，NTRU，SABER，CRYSTALS-DILITHIUM，FALCON）	次点候補に１方式が選定（SIDH）

SIDH：Supersingular Isogeny Diffie-Hellman

2. 格子暗号

2.1 格子暗号概要

格子暗号は，格子（線形独立なベクトルの整数線形結合で表されるベクトルの集合）に関する計算問題（格子問題）の解読困難性を安全性の根拠とする暗号技術である。この章では格子暗号の安全性の根拠になる様々な問題（Module LWE問題，NTRU問題，Module LWR（Learning With Rounding）問題など）が登場するが，問題によって異なるものの，それぞれが特殊な格子に関連する計算問題である。

NISTの耐量子計算機暗号標準化では，最も候補方式の数が多いのが格子暗号である。また，NISTは公開鍵暗号とデジタル署名について，格子暗号の候補方式の中から少なくとも一つずつは標準化方式として選出するであろうと明言しており，耐量子計算機暗号の標準化方式として非常に期待されている暗号技術である。

2.2 NIST標準化候補方式（格子暗号）

格子暗号の第3ラウンド候補は，最終候補としてCRYSTALS-KYBER，NTRU，SABER，CRYSTALS-DILITHIUM，FALCONの５種類の方式が選ばれており，次点候補としてFrodoKEM，NTRU Primeの２種類の方式が選ばれている。

(1) CRYSTALS-KYBER

CRYSTALS-KYBER方式はModule LWE問題と呼ばれる格子問題の解読困難性を安全性の根拠とする公開鍵暗号方式である。多くのアプリケーションで利用可能な効率性を達成しており，また，特定のパラメータを増減させるだけで効率性と安全性のトレードオフを容易に調整可能であるという特長を備える。

(2) NTRU

NTRU方式は，NTRU問題と呼ばれる格子問題の解読困難性を安全性の根拠とする公開鍵暗号方式である。NTRU問題は長い歴史を持つ格子問題であり，長い期間，安全性を精査されている。しかし，鍵生成が他の格子暗号方式に比べて低速であるという欠点がある。

(3) SABER

SABER方式は，Module LWR問題の解読困難性を安全性の根拠とする公開鍵暗号方式である。CRYSTALS-KYBER方式に匹敵する効率性を持つ。

(4) CRYSTALS-DILITHIUM

CRYSTALS-DILITHIUM方式は，Module LWE問題とModule SIS（Small Integer Solution）問題の解読困難性を安全性の根拠とするデジタル署名方式である。鍵サ

イズと署名サイズや，各種アルゴリズム（鍵生成，署名生成・検証）の効率性のバランスが取れているという特長を備える。

⑸ FALCON

FALCON方式は，NTRU問題の解読困難性を安全性の根拠とするデジタル署名方式である。署名生成と署名検証アルゴリズムは非常に効率的であるが，鍵生成アルゴリズムが低速であるという特徴を備える。一方で，公開鍵サイズと署名サイズの総和は，CRYSTALS-DILITHIUM方式よりも小さいという特長を持つ。

2.3 高安全なデジタル署名方式の構成

三菱電機では，2015年から格子暗号の研究開発に取り組んでいる。代表的な成果を次に簡単に述べる。これは格子問題を安全性の根拠とするデジタル署名方式の高安全化に寄与する成果である。

LWE問題，Module LWE問題，Ring-LWE問題など，格子暗号には様々な格子問題が存在し，それらは問題で使用される格子を定義する多項式による違いがある。特定の多項式を用いることで処理速度が向上することなどが知られる一方で，安全性の低下を招くおそれがあり，どのような多項式に対して構成するかは非常に重要である。そこで，Middle-product LWE問題と呼ばれる比較的新しい格子問題を安全性の根拠として高安全なデジタル署名方式を設計した。Middle-product LWE問題の解読困難性は，様々な多項式に関連して定義される格子問題の解読困難性の下で保証されるという性質を持つ。現在，格子暗号として利用されている暗号技術の安全性は，ある固定された多項式について定義される格子問題の解読困難性によって保証されているため，先に述べた安全性上の問題があるが，Middle-product LWE問題を使用することで，特定の多項式に関連して定義されていないような格子問題を安全性の根拠にできる，先に述べたリスクを回避した高安全なデジタル署名方式を構成できる[(2)]。

2.4 格子暗号の今後の展望

2023年までには，NISTによる標準化ドラフトの公開が予定されており，数年以内には標準化方式が策定される。どの格子暗号方式が標準化方式に策定されるにせよ，暗号技術を安全に運用するためには格子暗号に関する深い知見が必要不可欠であるため，研究開発を促進し格子暗号技術への理解を深めることが重要である。また，格子暗号で使用される技術は暗号化したままデータの情報処理が可能な準同型暗号への応用も期待されているため，次世代暗号技術の開発には非常に重要な技術である。

3. 同種写像暗号

3.1 楕円曲線暗号から同種写像暗号へ

素数pが与えられると，0から$p-1$までのp個の整数からなる和と積の定まった有限の数の世界$\mathbb{F}_p$を構成できる。これを標数pの有限体と呼ぶ。a，bを$\mathbb{F}_p$の元として方程式

$$Y^2 = X^3 + aX + b$$

を楕円曲線と呼ぶ。この楕円曲線上には楕円点$P_1=(x_1, y_1)$，$P_2=(x_2, y_2)$が存在し，これら楕円点に対して加算を定義できる。すなわち，二つの楕円点，$P_1=(x_1, y_1)$，$P_2=(x_2, y_2)$を与えると，三つ目の解$P_3=(x_3, y_3)$を$\mathbb{F}_p$上の演算を利用してx_1，y_1，x_2，y_2から計算ができる。加算が定義できるため楕円点は群（有利点群）を成して，この性質を利用して楕円曲線暗号は実現されている。楕円曲線での有理点群上の楕円離散対数問題を，現在の計算機で効率的に解くアルゴリズムは知られておらず，楕円曲線暗号の安全性の根拠になっている。しかし，楕円離散対数問題はShorのアルゴリズムによる大規模な量子コンピュータによって解読されてしまうことが分かっている。

このような状況に対して，量子コンピュータによる解読にも耐え得る楕円曲線の数論を用いた新たな暗号方式の研究が進められている。それは楕円曲線の同種写像を基礎に置く暗号方式群であり，同種写像暗号と総称される。同種写像とは複数の楕円曲線間の代数的な表現を持つ群準同型写像のことである。一つの楕円曲線E_1が与えられたとき，その有限部分群Gを一つランダムに選ぶと，それに対応した同種写像とその像$f_G : E_1 \rightarrow E_2$が定まり，かつ計算が可能である。一方で，楕円曲線$E_1$と$E_2$が与えられたとき，それらの間の同種写像に対応する$E_1$の有限部分群$G$を計算することは計算量的に困難な問題であると考えられている。この問題を同種写像問題という。同種写像暗号のアイデアの核心は，同種写像の像の情報E_2を公開鍵に利用し，E_1からE_2への同種写像を与える有限部分群Gの情報を秘密鍵に利用するというものである。

3.2 同種写像暗号方式とNIST標準化候補方式

重要な同種写像暗号方式として2011年に提案されたSIDHと2018年に提案されたCSIDH（Commutative SIDH）がある。どちらも格子暗号に比べると効率性は劣るが，鍵サイズが著しく小さい鍵共有方式になっている（**表1**）。例えば，SIDHの公開鍵のサイズは330バイト程度であり，CSIDHでは64バイトである。CSIDHはNISTによる耐量子計算機暗号の標準化が始まった後の提案であったが，SIDHはこれを基にした暗号化であるSIKE（Supersingular

Isogeny Key Encapsulation)が標準化に投稿されて第3ラウンドの次点候補になっている。

格子暗号を含めた他の耐量子計算機暗号では鍵サイズや暗号文サイズの小さい暗号化方式を構成することは難しいため，SIKEは有望な方式の一つである。しかし，効率性及び安全性の面に課題を抱える。効率性に関しては，暗号化に同種写像計算という複雑な処理が必要であり，格子暗号と比較して暗号化が10倍程度低速という問題がある。安全性に関しては，同種写像暗号は提案から10年程度しか経(た)っていないという点から，数学的な研究及び解析が研究途上であるという点に問題がある。したがって，今後同種写像暗号を実用していくためには，同種写像計算の数学への深い理解とそれによる計算の効率化及び同種写像問題への様々な数学的アプローチによる理解が必須になる。

3.3 同種写像暗号に関する安全性と効率性解析

当社では，同種写像暗号の安全性や効率性の解析を行っている。まず，安全性に関して，四元代数と呼ばれる代数的構造を利用した解析を行った。楕円曲線とある四元代数の極大オーダーが一対一に対応するというドイリング対応というものが存在する。これの対応を用いて，四元代数側で同種写像の対応物を計算し，それを楕円曲線側に戻して同種写像問題を解くアルゴリズムを構成することで安全性解析を行うというものである。前者を解く数論アルゴリズムとしてKLPTアルゴリズムが，後者を解く数論アルゴリズムとして構成的ドイリング対応アルゴリズムが知られている。まずKLPTアルゴリズムの性能向上を行い，さらに，その結果を構成的ドイリング対応アルゴリズムの性能向上へ応用した。その結果，従来10ビット標数の有限体上での動作が限界であったが25ビット標数での実装例を構成した[3]。これは今後，安全な同種写像暗号のビット長を選定する際に考慮すべき結果になると考えられる。

効率性に関して，これまで様々なタイプの楕円曲線に対して個々に同種写像計算公式が構成され，それらの間の実装性能比較が行われてきたが，どの計算方式を利用しても数％程度の性能差しかないことが知られていた。そこで，これまで個々の楕円曲線に応じて調べられてきた同種写像計算を統一する理論的枠組み(一般化モンゴメリー座標の理論)を構築し，それを用いて一般の楕円曲線に適用できる公式を導いた。この公式は既存研究の多くを含んで，更に一般化を行い既存研究で示された“公式間の性能差は数％程度”という事実を数学的に説明することに成功した。つまり，この結果は同種写像計算が特別高速になるような楕円曲線のタイプは存在しないということの一つの証拠を与えた[4]。

3.4 同種写像暗号の今後の展望

2010年頃から研究が始まった同種写像暗号は，このように数学と深く交わりながら著しく発展を続けている。実用化へ向けて特に重要な研究は安全性解析であり，暗号の安全性を保証するために様々な数学的技術を駆使した解析及び実装データ収集が求められる。処理の効率性に関しては，同種写像計算という重い処理を含むため抜本的な進展を得ることは難しいように思われるが，データサイズが小さいという強みを生かしたユースケースの検討も考えられ，そのためのデータサイズ圧縮技術の研究なども重要になる。また，同種写像暗号の欠点の一つに代数性の乏しさがあり，それによって格子暗号のように高い機能を暗号方式に持たせることが難しい。今後，同種写像暗号の高機能化の研究も重要性が増していくものと思われる。

4. む す び

量子コンピュータに対しても解読耐性のある耐量子計算機暗号のうち，格子暗号と同種写像暗号に関してその概要と，格子暗号について高安全なデジタル署名方式を，同種写像暗号について安全性解析の改良と効率性に関する証拠を述べた。

今後も安全性解析と設計とを行い，安心・安全な社会の実現に貢献していく。

参 考 文 献

(1) NIST：Post-Quantum Cryptography
https://csrc.nist.gov/Projects/post-quantum-cryptography

(2) Bai，S.，et al.：MPSign: A Signature from Small-Secret Middle-Product Learning with Errors，PKC 2020，66～93 (2020)

(3) Kambe，Y.，et al.：Solving the Constructive Deuring Correspondence via the Kohel-Lauter-Petit-Tignol Algorithm，Mathematical Cryptology，**1**，No.2，10～24 (2021)

(4) Moriya，T.，et al.：The Generalized Montgomery Coordinate: A New Computational Tool for Isogeny-based Cryptography，IACR Cryptology ePrint Archive，**2022**，150 (2022)

特集論文

LSI開発の下流工程での性能・回路規模・消費電力改善技術

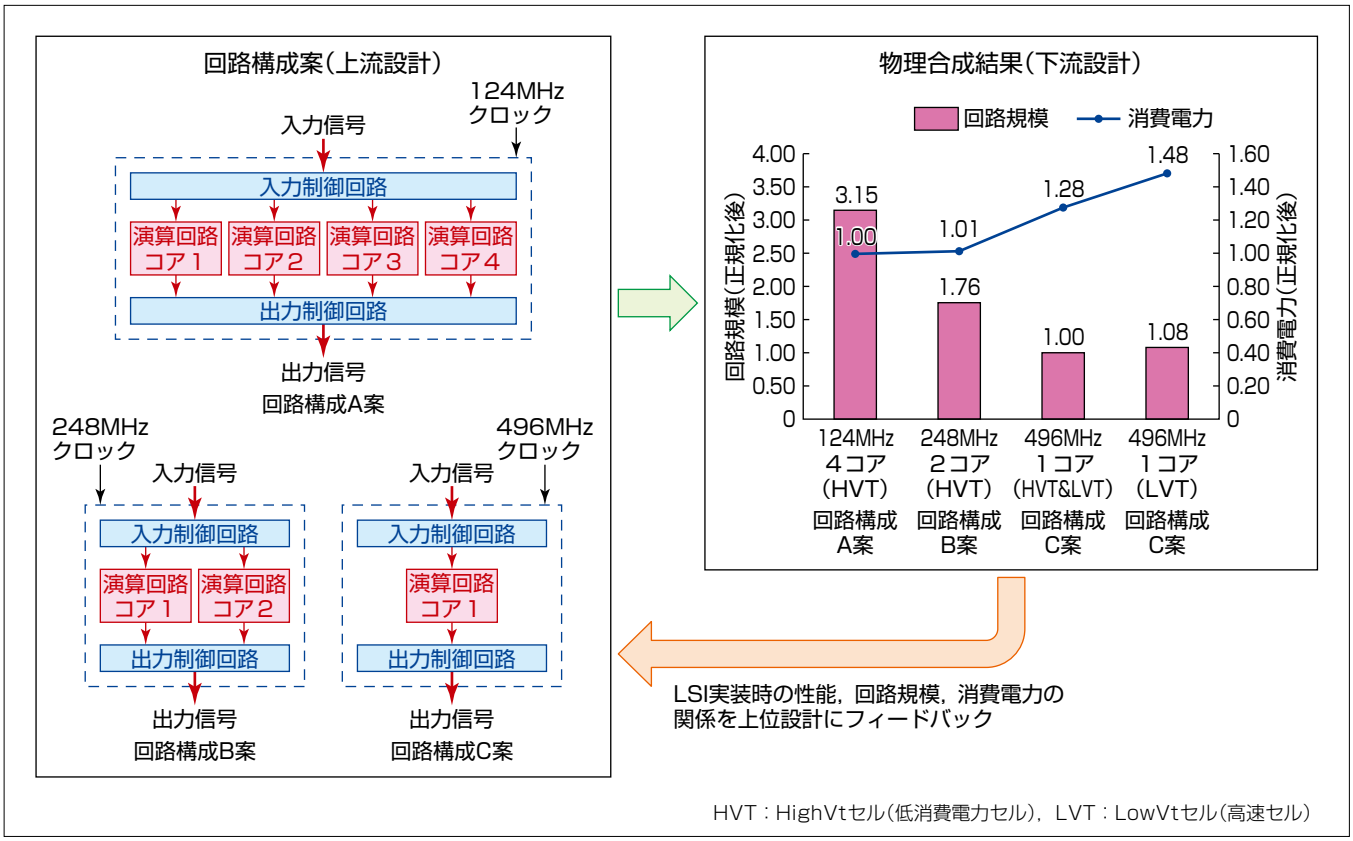
平野　進*
Susumu Hirano
小川吉大*
Yoshihiro Ogawa

Design Technology for Improving Performance, Circuit Scale, and Power Consumption in the Backend Phase of LSI Development

要　旨

持続可能な社会の実現に向けて，情報技術によって複雑な問題を限られたエネルギーで解決する必要があり，機器には高機能化と省エネルギー化の両立が求められている。これを実現する手段の一つとしてLSI化があり，半導体のプロセス微細化によって，回路高速化や１チップの回路規模搭載量増加，消費電力削減が可能になったが，一方で，プロセス微細化が進むにつれて配線遅延・混雑，トランジスタ特性のばらつき，リーク電流等の新たな問題も発生してきている。これらの問題に対応するために，LSI開発の下流工程(レイアウト設計)を考慮した，性能・回路規模・消費電力の改善技術が求められる。

近年の微細化プロセスの恩恵を十分に得るためには，従来の設計とは異なる設計手法を取り入れていかなければならないことが分かってきた。従来の設計フローでは，回路設計した後に下流工程を行う一方通行の流れであったが，近年の微細化プロセスでは，上流設計の中で下流工程の一部(配置配線を考慮した物理合成等)を事前に行い，その結果に応じて上流設計の指針を随時変更していくことが必要である。特に，性能向上・回路規模削減・消費電力削減では，複雑なトレードオフ関係があり，従来下流工程で行っていたクリティカルパス削減，階層設計，電源電圧低減／停止等への対応策を上流工程から考慮した回路設計と回路実装の最適化アプローチが重要である。



HVT：HighVtセル(低消費電力セル)，LVT：LowVtセル(高速セル)

プロセスに応じた設計：性能(動作周波数)，回路規模(面積)及び消費電力の関係

微細化プロセスを用いたLSI設計では，その実力を最大限に引き出すため，プロセス特性に応じた，動作周波数，回路規模及び消費電力のトレードオフの複雑な関係を上流設計時点から把握し，設計指針を規定してフロントローディングを行うことが重要である。図の場合，同一性能を実現するために，回路規模と消費電力のどちらを重視するかによって回路構成を決めなければならない。

*情報技術総合研究所

1. ま え が き

持続可能な社会の実現に向けて，情報技術によって複雑な問題を限られたエネルギーで解決する必要があり，機器には高機能化と省エネルギー化の両立が求められている。これを実現する手段の一つとしてLSI(ASIC(Application Specific Integrated Circuit)，FPGA(Field Programmable Gate Array))がある。

LSIは必要な処理だけを，処理に応じた効率的な回路構造で実装でき，回路領域を少なくして無駄なく処理を行えるようになるため，小型化を可能にするだけでなく，エネルギー効率も良くなって，消費電力を低く抑えることで省エネルギーへの貢献も期待できる。

LSIは高機能化に対応するためにムーアの法則で知られるようにプロセステクノロジーが進化し，プロセス微細化が進んでその集積量を増やしてきた。また，デナード則による“微細化＝高速・省電力化”で，高性能化，低消費電力化の要求にも対応してきた。

これまでは，プロセステクノロジーの進化に伴い，LSIの実装ツール(論理合成ツールやレイアウト設計ツール)も進化し，LSI回路設計者はLSIの実装ツールに任せておけば微細化プロセスで所望の性能や電力を得ることができていた。しかし，近年の微細化プロセスは従来と比較して複雑化し，配線混雑，チップ内のタイミングばらつき，リーク電流等の新しい問題が出てきており，LSIの実装ツールを適切に使いこなさないと微細化プロセスの恩恵を十分に得られないだけでなく，LSIの実装ができず，開発遅延のリスクにもつながるようになってきている[(1)]。

2. 近年の微細化プロセスと設計の傾向

これまでの微細化プロセスでは，上流設計の回路設計者は性能を出すために，動作周波数を可能な限り上げるか，動作周波数が上限に達した場合は回路を並列化するだけでよかった。そして，下流設計者は市販の回路実装ツールを用いて論理合成やレイアウト設計を実施する，という一方通行の設計の流れであった。

近年の微細化プロセスでは，高速化の対策としてLVTがある。このセルは電流を多く流すことで高速化を実現しているが，リーク電流(動作に関係なく流れる電流)によって消費電力が増加するというデメリットがある。

一方，低消費電力なセルとしてHVTがあるが，LVTと比較して速度の面でデメリットがある。

つまり，下流設計では性能(動作周波数)と回路規模(面積)・消費電力のトレードオフ関係を考慮してセルを選ぶ必要がある。

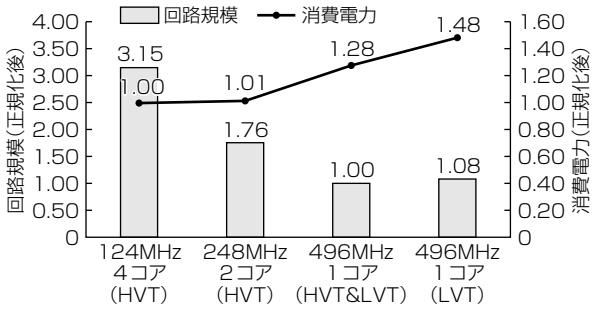


図1．動作周波数，回路規模及び消費電力の関係

図1は配線数が多い回路での物理合成(配置配線を考慮した論理合成)結果についてまとめたものである。同一性能を実現するために，動作周波数の高いLVTを使用して性能を達成する方法と，動作周波数の低いHVTを使用して回路並列化(コア数を増加)することで回路規模を増やして性能を達成する方法との，消費電力の関係を比較している。

248MHz/2コア(HVT)と，496MHz/1コア(HVT&LVT)を比較すると，前者は消費電力が27%低く，後者は回路規模が76%少ないことが分かる。つまり，その開発で消費電力と回路規模のどちらを優先するかによって，回路の設計方法が変わることになり，回路実装結果を考慮しないと回路設計ができないということになる。

さらに，近年の微細化プロセスではチップ内の一つ一つのセル(基本回路ライブラリ)は微細化によって高速化されているが，プロセス(製造のばらつき)，電圧，温度によって，回路の遅延が変動したり，性能に対する配線遅延の影響比率が増えたりするようになり，高速化のためには考慮すべき条件が多く複雑になっている。また，プロセスルール(16nmプロセス，5nmプロセス等)によっても条件が変わるため，同一の回路でもプロセスルールが変われば動作周波数や回路構成を見直す必要がある。

つまり従来のような一方通行の設計の流れでは，目標とする性能，回路規模，消費電力を実現することはできない。

3. 微細化プロセスに向けた設計手法

近年の微細化プロセスを用いたLSI開発では，下流設計で大きな手戻り(目標とする性能，回路規模，消費電力を実現できずに回路の大改修を行うなど)が発生しないようにするために，上流設計の時点から下流設計工程を考慮した回路設計を行うことが必須になってきている。速度改善，回路規模削減，消費電力削減のそれぞれ目的別の手法を次に示す。

3.1 速度改善手法

2章で述べたように速度改善にはLVTを活用すること

が有効であるが，LVTの活用は消費電力増加を招くことになる。そのため，安易なLVTの使用は避けて，必要最低限の使用にとどめることが重要である。そのためには，まず細かい単位でLVTを指定できるようにする必要がある。セルの指定はブロック単位で行う必要があるため，回路設計の時点で各ブロックを細かい単位（1 MG（ミリオンゲート）以下推奨）になるように，ブロック分割・サブブロック分割を行っておく必要がある。

次にLVT以外の方法での速度改善も有効である。微細化による実装可能な回路量の増加に伴い，回路間の配線数も多くなり配線混雑が発生する。配線混雑の発生は迂回（うかい）配線の発生につながって，迂回配線によって配線長が長くなり速度が出ないという結果になる。配線混雑はタイミング条件の厳しい配線が集中することから発生するため，タイミング条件が厳しいパスを減らすことが重要になる。それには機能的に1サイクルで到達しなくてもよいパスには回路設計の時点でFF（フリップフロップ）を入れたり，マルチサイクルパス（物理合成の際に必要なサイクル数）を設定したりすることでタイミング条件を緩和することが可能である。また，配線集中の発生を避けるために，ファンアウト数の多い回路設計を控える，多入力セルの使用を控える，大容量SRAM（Static Random Access Memory）を分割するなどの方法が効果的である。

このような方法を行い，真のクリティカルパスになる箇所を抽出してLVTを使うことで，消費電力とのトレードオフを図ることが可能になる。

3. 2　回路規模削減手法

回路規模削減に関しては下流設計ツール（物理合成・レイアウト設計ツール）の実装最適化機能に任せることが有効であるが，微細化によって下流設計ツールの機能だけでは効果的な回路規模削減ができなくなってきている。その一番の要因はLSIに実装できる回路規模が膨大になってきたことである。プロセスが1/2，1/3，…と微細化すると同一面積に実装できる回路規模は4倍，9倍，…と2乗で増えてくる。回路規模の増大は配線数の増大につながり，配線方法の組合せは更に増えて，複雑になってくる。その複雑度は，下流設計ツールの進化以上に進んで，従来のトップダウン設計手法のように大規模回路をまとめて下流設計ツールにかけると，非現実的なツール実行の長時間化や，最適化ができずに回路規模が増大するような結果になってしまう。

そのため，回路設計の時点でブロックを小さい単位（数MG以下推奨）になるようにブロック分割し，ブロックごとに下流設計ツールで最適化を行い，その結果を積み上げていくボトムアップ設計手法が必要になってきている。しかし，単にブロック分割すればよいわけではなく，ボトムアップで積み上げていったときに回路規模削減可能な最適配置を考慮したブロック分割が必要である。

ブロック分割で考慮すべきことの一つ目としては，ブロックのピンペア数（回路規模に対する入出力ピン数）がある。極端にピン数が多い場合，ブロックサイズがピン数だけで決まってしまい，ブロック内の回路占有率（面積に対する回路実装率）が低くなり，ブロックの回路規模が増えてしまうことがある。そのため，ピン数が偏らないようなブロック分割を推奨している。

考慮すべきことの二つ目としては，配線混雑である。配線混雑は**3. 1節**の速度改善手法で述べたような不必要な迂回配線が発生するだけでなく，配線のタイミング条件を満たすために回路配置が制限され，ブロック内の回路占有率が低くなる要因になる。配線混雑を避けるためには，**3. 1節**の速度改善で述べた手法が有効であるが，仮にその配線混雑を避ける対応で上流設計上の回路が増えたとしても，配線混雑度を減らすことによって下流設計後の回路規模が減る可能性は高い。

考慮すべきことの三つ目としては，信号の流れを考慮したブロック分割である。ボトムアップで最適化したブロックは最終的に手置き配置でレイアウトを行うことになるため，入力ピンから出力ピンまでの信号の流れに合わせてブロックを配置していった場合に，回路規模増加の要因になるブロック間の複雑な配線や不規則な配線を作らないようにブロック分割をすることが重要である。また，上流設計のブロック分割で目標の回路規模が実現できない場合，下流設計でブロック分割・統合を行い，階層変更をして下流設計ツールを実行することがあり，この手法によって上流設計に手戻りを発生させないようにすることが可能である。ブロック分割・統合をしやすい回路構成の例を**図2**に示す。

図2では，ブロックの階層直下はセル置き不可，サブブロック（黄色部分）の入出力にはFFを挿入するなどの構造化記述を行っており，ブロック分割・統合容易化だけでなくサブブロック単体だけで（接続先に関係なく）タイミング判断できるようになるというメリットもある。

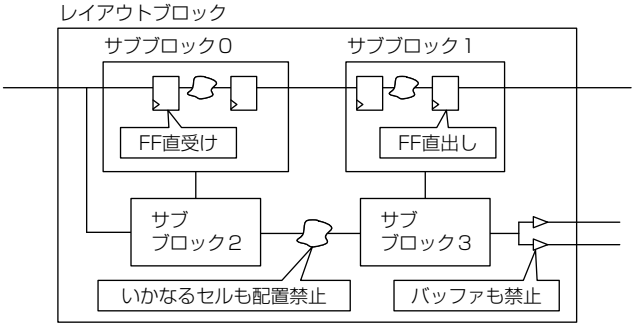


図2．レイアウト設計に優しい回路構成

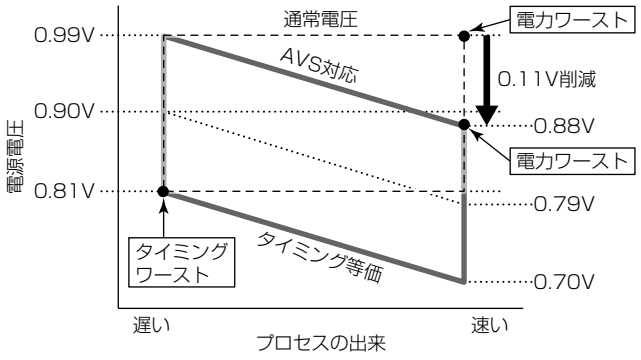


図3．AVSの電源電圧可変イメージ

3.3　消費電力削減手法

近年の微細化プロセスの消費電力削減で有効な手段の一つがAVS(Adaptive Voltage Scaling)手法[2]である(**図3**)。LSIの製造上のばらつきや周囲温度によってLSIの動作を保証する最低電圧を変化させることで消費電力削減効果を上げている。AVSの適用箇所は下流設計で判断するが，AVSはタイミングが厳しいパスが存在する回路では電源電圧が下げられず消費電力削減効果が低下するため，回路設計段階からクリティカルパスを発生させないように考慮しておく必要がある。

以前から行われてきた消費電力削減手段として，動作不要な回路のクロック供給を停止することで消費電力を削減する，クロックゲーティング手法がある。クロックゲーティングは下流設計ツールで自動的に回路変更をすることで実現が可能である(信号の遷移が少ないパスにイネーブル信号を付与し信号遷移時だけFFにデータを取り込むようにすることで，論理合成時に信号遷移以外の期間はクロックを止めるよう回路変更する)。しかし，近年の微細化プロセスはクロックゲーティングではリーク電力が下がらないために消費電力削減効果が上がらなくなってきている。

これに対して，回路が動作しない期間はそのブロックの電源を切る，パワーゲーティング手法が近年は主流になってきている。同様に，電源電圧をロジックセルのように下げられずAVS対象外になることがあるSRAMにはパワーゲーティングは有効な電力削減手法であり，SRAMは独自のパワーゲーティング機能が付いているものが増えてきている。

パワーゲーティング手法を使うには回路のブロック単位で動作を停止する期間と停止期間中に他の回路に影響をしない回路構造である必要があり，上流設計の段階からパワーゲーティングを考慮した回路設計が必要である。

また，従来と比較して基本的な電力削減に向けた回路設計指針も変わってきている。従来は回路のFF数を極力減らして回路自体を減らすことで消費電力を減らす手法が一般的であった。しかし，近年の微細化プロセスでは，組合せ回路にLVTを使うことの方が消費電力増加への影響が多いことから，パイプラインFFを挿入することで，クリティカルパスを回避したり配線混雑を緩和したりした方が総合的に消費電力を削減できるように変わってきている。

4．微細化プロセスに向けた設計フローの変化

3章で述べたように，微細化プロセスに向けた設計手法は従来とは変わってきており，下流設計のLSI実装を考慮して上流設計をすることが重要である。

3章で述べた設計手法を適用するためには，上流設計開始前に設計指針を規定しフロントローディングを行うことが必要である。しかし，上流設計の段階で**3章**に述べた内容を全て考慮することは非常に困難であり，方針を見誤ると大きな手戻りへとつながる。そのため，三菱電機は上流設計の途中段階(回路のコーディングが終わって論理検証をする前)で下流設計工程の一部である物理合成やレイアウト設計を行い，回路設計に設計方針の補正等のフィードバックを行う設計フローに変化させる必要があると考えている。

5．む　す　び

本稿では，近年の半導体微細化プロセスでのLSI設計技術について，LSI開発の下流工程を考慮した性能・回路規模・消費電力の改善技術について述べた。

微細化プロセスの恩恵を十分に得るためには，従来の設計とは異なる設計手法も取り入れていかなければならないことが分かってきた。特に，速度改善と回路規模削減及び消費電力削減では，より複雑なトレードオフ関係が見えてきており，**3章**，**4章**で述べたような上流設計からの実装最適化アプローチが重要である。今後はプロセスに応じた設計を行わないと最適解は見出せず，流用回路であっても設計を見直す必要があることを認識しておくべきである。

本稿では当社の設計手法という観点で述べてきたが，下流設計を担当するASICベンダーの選定も重要である。微細化プロセスの経験の少ないベンダーだと工程長期化や電力削減手法の実施不可等があり所望のLSIが実現できない事態に陥る可能性もあることに注意が必要である。

また，本稿では主にASIC開発について述べたが，微細化プロセスの影響はFPGAでも同様であり，今回提案した設計手法はFPGA設計でも有効である。

参 考 文 献

(1)　平野　進，ほか：光通信用LSI開発にみる微細化プロセスの対策技術，VLSI設計技術研究会，**118**，No.457，VLD2018-110，103～108 (2019)
(2)　JEITA半導体技術ロードマップ専門委員会(STRJ)設計ワーキンググループ(WG1)：SOCの低消費電力設計技術の課題と解決策，STRJ WS，22 (2009)
https://semicon.jeita.or.jp/STRJ/STRJ/2008/5B_Design.pdf