第２部
情報基盤研究開発センター活動報告

第１章　応用データ科学研究部門
第２章　教育情報基盤研究部門
第３章　先端サイバーネットワーク研究部門
第４章　先端計算科学研究部門
第５章　情報システムセキュリティ研究部門
第６章　汎オミクス計測・計算科学センター

第７章　研究報告

7.1　小野　謙二〈応用データ科学研究部門 教授〉
7.2　内林　俊洋〈応用データ科学研究部門 助教〉
7.3　谷口　雄太〈教育情報基盤研究部門 准教授〉
7.4　石　偉〈教育情報基盤研究部門 助教〉
7.5　岡村　耕二〈先端サイバーネットワーク研究部門 教授〉
7.6　笠原　義晃〈先端サイバーネットワーク研部門 助教〉
7.7　美添　一樹〈先端計算科学研究部門 教授〉
7.8　渡部　善隆〈先端計算科学研究部門 准教授〉
7.9　南里　豪志〈先端計算科学研究部門 准教授〉
7.10　大島　聡史〈先端計算科学研究部門 准教授〉
7.11　樋口　祐次〈先端計算科学研究部門 准教授〉
7.12　小 出　洋〈情報システムセキュリティ研究部門 教授〉
7.13　櫻井　大督〈汎オミクス計測・計算科学センター 准教授〉

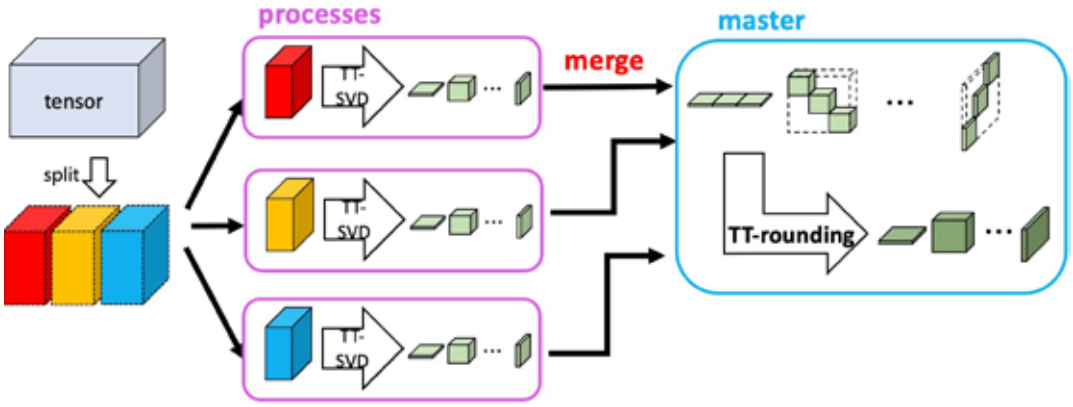
第８章　イベント紹介

第 7 章　研究報告

7.1　小野　謙二　〈応用データ科学研究部門 教授〉

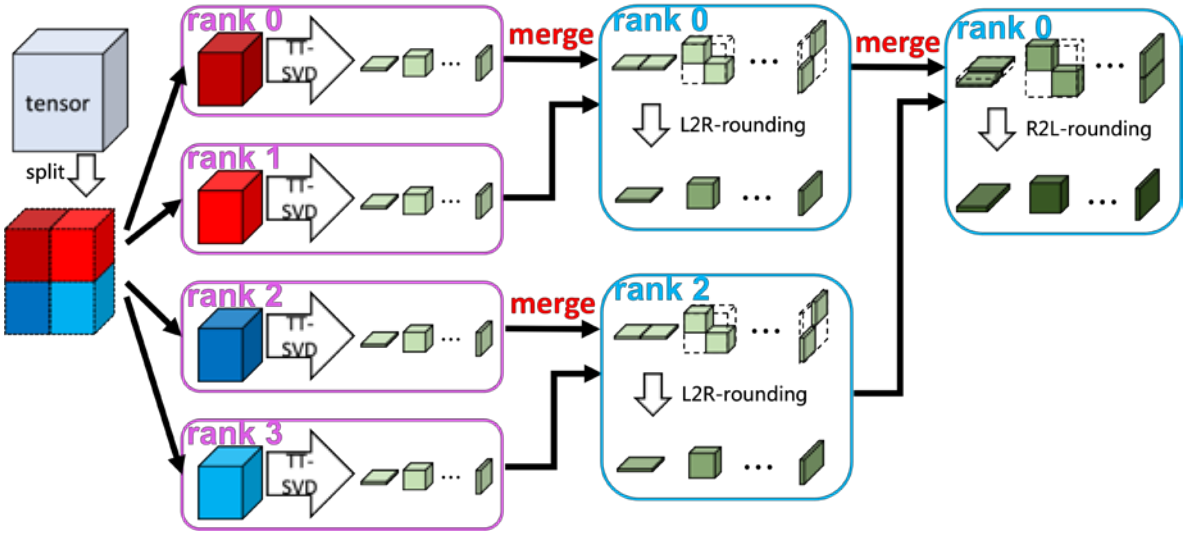
高次元データのテンソルトレイン分解

計測や数値解析、機械学習など様々な分野で高次元配列データが現れ、その解析の必要性が高まっている。近年、空間量 $O(n^d)$ をもつ階数 d、次元数 n の高次元テンソルを $O(dnr^2)$ の分解形に圧縮するテンソルトレイン分解（TT 分解）が提案され、注目されている。ここで r は特異値分解（SVD）を適用した場合のランク数である。テンソルトレイン分解アルゴリズムで用いられている TT-SVD は逐次計算であるため、膨大な計算時間と使用メモリ量を要する点が課題となっている。この問題点を改善するため、領域分割的アプローチを用い、TT 分解を分散並列処理するアルゴリズム PTTD を開発してきた。PTTD はテンソルをいくつかの小さいテンソルに分割してノードに割り当て、並列に TT 分解した後、それらをマージして元のテンソルの TT-format を求めるというアルゴリズムである。分割数 M が小さい場合は時間計算量が 1/M 程度になる非常に優秀な手法であるが、Rounding 処理は時間計算量が O（M^3）に比例するのため、分割数が大きい場合にはボトルネックとなる【図 1】。



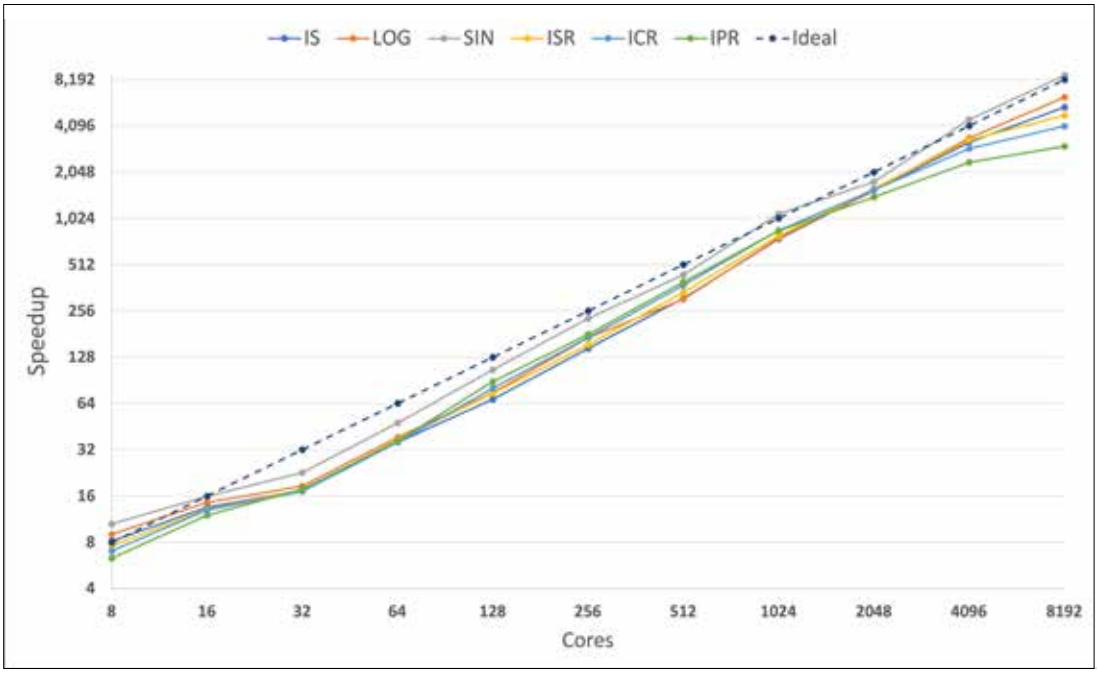
【図 1】　PTTD アルゴリズム

Rounding 処理には QR 分解と特異値分解で構成される TT-Rounding という手法が用いられてきたが、本研究ではその中の QR 分解を省くアルゴリズムに加えて、並列に Rounding 処理を行うことにより、計算時間を削減するアルゴリズムを提案した【図 2】。



【図 2】　提案した改良版の PTTD アルゴリズム

数値実験を九州大学情報基盤研究開発センターのスーパーコンピューターシステム ITO で行った。ITO は 1 ノードに 18 コアの Intel Xeon Gold 6154(Skylake-SP)2 つと 96GB のメモリー 2 つを搭載しているが、実験ではフラット MPI を用い 1 ノード 32 コアまでを使用した。実験はランク数が低いことで知られている 6 種類のテンソル（IS、LOG、SIN、ISR、ICR、IPR）に対して並列数を変えて分解した。図 3 には、提案する改善アルゴリズムで 8192 並列までのスピードアップ率を示す。いずれのテンソルデータに対してもスケーラブルな性能が得られていることがわかる。



【図 3】　NOQR-rounding を用いた PTTD の高速化率
Ideal は高速化率と並列数が一緒である場合 を示している

本研究によって改善された PTTD は、分解でできた TT-format の空間使用量が逐次アルゴリズム TT-SVD よりすこし大きいが、決定的手法（乱択アルゴリズム以外）の TT 分解の並列アルゴリズムの中で最も良い性能を示した。乱択アルゴリズムは性能が良いが、誤差をコントロールできない問題点がある。本提案アルゴリズムは、誤差を指定された閾値以下に抑えられる点や任意の次元軸に分散されたテンソルを分解できる点などのメリットがある。

7.2　内林　俊洋〈応用データ科学研究部門 助教〉

地域公共交通向け従業員管理支援システムの構築

都市部から離れるにつれて人口が減るため、公共交通機関の多様性が一気に薄まる。特に高齢者の多い地域には死活問題である。地方自治体はこの問題を解決するために、地方自治体の財源を主としたコミュニティバスなどの公共交通機関を運行し始めている。高齢者の主な移動手段は公共交通機関であるため、公共交通機関がなくなることは生命活動の危機に直結する。つまり、日本国内に公共交通機関の空白地帯があってはならず､なんとしても交通網を維持しなければいけない。また、地域公共交通では、運転手のなりて不足と高齢化が日に日に問題となっている。

地域公共交通

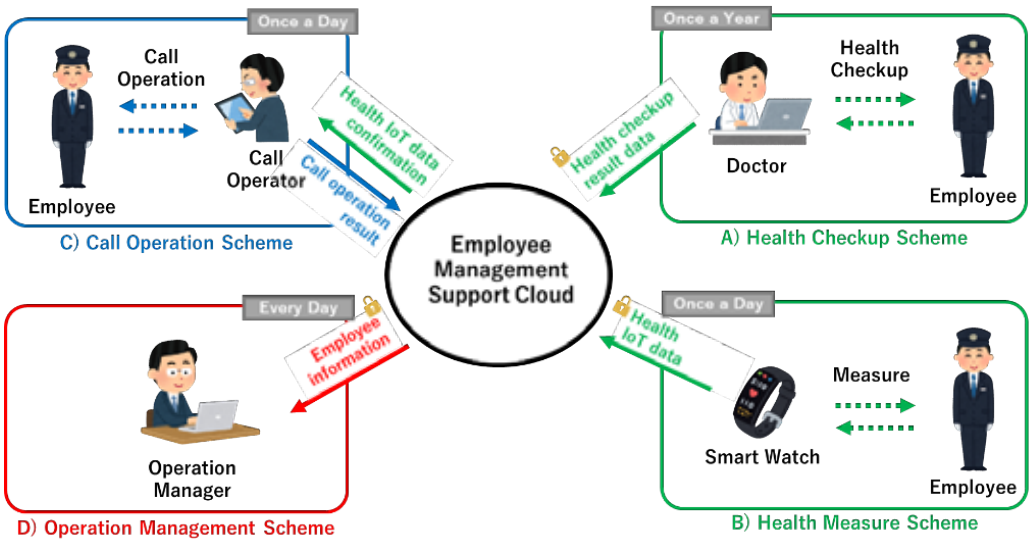
以前の日本の地方公共交通は、主に民間企業や公益法人によって管理・運営され、管理・運営コストの大半を乗客が支払う運賃で賄っている独立採算制であった。しかし、民間企業の独立採算制が厳しくなるに従って、財政的に独立した民営バスではなく政府が多額の補助金を配分するような公営バスへと移行していった。そのため、地域公共交通の多くは、主要交通機関が撤退した過疎地域や主要交通機関が運行しない隙間地域を埋めるために運行されている。

さらに、地域公共交通を経営・運行するための財源の多くは地方自治体から補填されているため、慢性的な財政不足となっており、そのため、十分な人材の確保が金銭的に厳しく、限られた人員で地域公共交通の運行を継続している。日本の警視庁の統計によると、乗客 (旅客) を運ぶ目的でバス、タクシー、ハイヤー、そして民間救急車を運転する時に必要となる免許である第 2 種免許保有者数は年々減少している。2008 年には約 110 万人いた免許保有者は、2018 年には約 90 万人になっており、約 80% 減少している。さらに、前述の影響で最新の機材などを揃えることは厳しく、人員不足の中で運行管理などを未だに紙ベースで行うことが多く、業務過多となり負担となっている。

また、日本の従業員の高齢化が進んでおり、厚生労働省の賃金構造基本統計調査では、バスの運転手平均年齢は年々上昇しており、2010 年度では 46.5 歳であったのに対して、2019 年度では平均 50.7 歳である。これは企業規模が小さくなるほど従業員の高齢化が顕著となっており、平均年齢が高くなる傾向である。特に地域公共交通の多くは、他の企業規模に比べて大幅に高齢化が進んでいる。国土交通省の報告によると、事業用自動車において健康状態に起因する事故報告件数は増加傾向であり、2017 年度は約 300 件の報告があった。その中の約 3 割は、運転中に操作不能となっている。

システムの設計

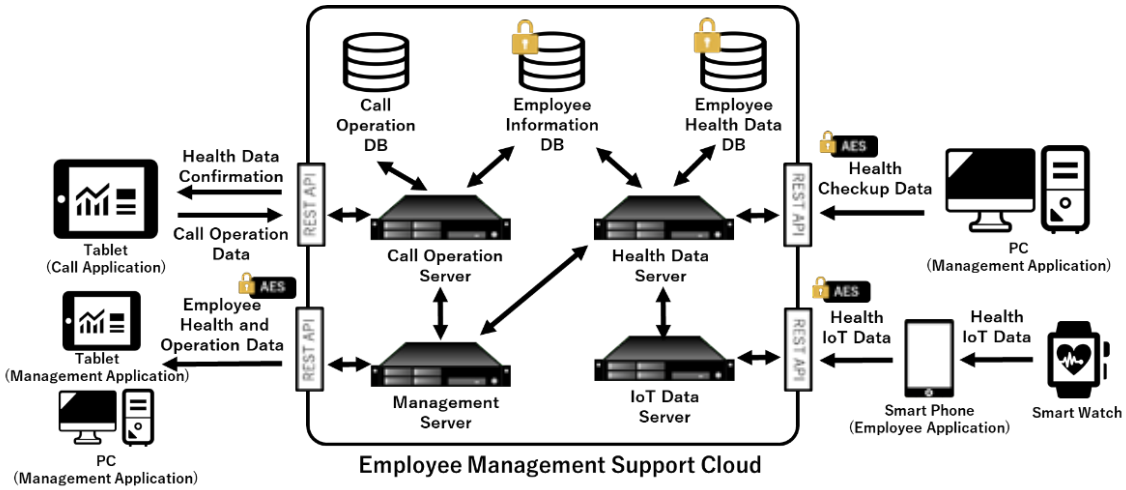
これらの問題を解決するために、地方公共交通向けの従業員管理システムの提案を行う【図 1】。このシステムは運行管理者･点呼者･医者･従業員が使うアプリケーションとこれらのアプリケーションと連携するクラウドで構成される。アプリケーションとクラウドの関係を図に示す。医者は従業員を対象とした年 1 回の定期健康診断の結果をアプリケーションから登録する。従業員は業務時にスマートウォッチを付け、スマートフォンのアプリケーション経由で 1 日 1 回健康データを提出する。点呼者は毎日の点呼業務で従業員が健康データを提出している場合のみ点呼作業を実施し、点呼内容を登録する。運行管理者はこれらのすべての経緯をアプリケーションで確認することができ、クラウドに集約された情報を考慮した運行管理業務を行う。



【図 1】　地方公共交通向けの従業員管理システムの提案

健康情報に関連するデータはパーソナルデータに帰属する機微情報であるため、クラウドと通信する際はデータを暗号化し、情報を秘匿する必要がある。具体的には AES256 で暗号化する。暗号と復号はシステムで利用する各アプリケーションで行い、ネットワーク上では素のデータを流さない。また、Date は DB 内の検索に使用するために、暗号化せずにクラウドへ送られ保管される。

クラウド及びアプリケーションの構成を【図２】に示す。クラウドは４つのサーバと３つのデータベースで構成される。Call Operation Server は、点呼者向けアプリケーションとの通信を受け持つ。アプリケーションへは点呼者と点呼される従業員の認証、従業員の健康 IoT データ提出の有無、そして点呼結果を受け取る。Management Server は、管理者向けアプリケーションとの通信を受け持ち、必要な情報をデータベースと受け渡しする。Health Data Server は、健康診断結果の管理を行う。医者が入力した健康診断の結果を受け取る。IoT Data Server は、従業員のスマートフォンから送られてくる健康 IoT データを受け取る。Call Operation DB は、点呼業務結果を保管する。Employee Information DB は、健康に関するデータを除いた従業員の情報を保管する。Employee Health Data DB は、健康診断結果と健康 IoT データなど、従業員の健康に関するデータを保管する。クラウドは REST API を提供し、アプリケーションとクラウドの通信はすべて REST API 経由で行われる。また、個人情報やパーソナルデータはアプリケーションですべて暗号化した後に通信するため、クラウドでは暗号化済みのデータしか保管しないものとする。



【図 2】　従業員管理システムの構成図

実装

3 つのアプリケーションは、すべて Flutter2.1.3 で実装している。Flutter は google が開発したフレームワークであり、マルチプラットフォームに対応している。今回は iOS と Android 向けにビルドを行っている。画面のキャプチャは iOS で実行したものである。点呼者向けアプリケーションは、タブレット向けのアプリケーションであり、iPad Air 2021 にて稼働させた。管理者向けアプリケーションは、タブレット向けのアプリケーションであり、同様に iPad Air 2021 にて稼働させた。従業員向けアプリケーションはスマートフォン向けアプリケーションであり、iPhone X にて稼働させた。また、Apple Watch 6 は従業員向けアプリケーションが稼働している iPhone X とペアリングしている。Apple Watch 6 で収集した計測データは iPhone X のヘルスケアに蓄積され、従業員向けアプリケーションはヘルスケアに蓄積されたデータをクラウドへ送信する。クラウドを AWS 上に構築する。システムで提案された各サーバと各 DB を AWS のサービスに置き換え実装する。各サーバを Lambda(Python) で実装する。各 DB は DynamoDB にて実装する。REST API は API Gateway で実装する。役割に応じて API Gateway と Lambda を 1 セットとし、必要に応じて Lambda から Dynamo DB へアクセスする。今回の実装では、点呼者の使用する点呼者向けアプリケーション、管理者の使用する管理者向けアプリケーション、医者の使用する管理者向けアプリケーション、そして、従業員の使用する従業員向けアプリケーションの 4 セットを実装した。例えば、点呼者向けアプリケーションから送られてくる点呼情報は、JSON 形式のデータとして API Gateway 経由で Call Operation Server に該当する Lambda に送られる。Lambda では送られてきた JSON を解析及び整理し、Call Operation Server に該当する Dynamo DB に保管される。

まとめ

地域公共交通における人員不足と従業員の高齢化の問題を解決するために、乗務前後の点呼の最適化、運行管理情報の過多による業務圧迫の改善、そして従業員の健康情報と運行管理情報の連携に着目した。

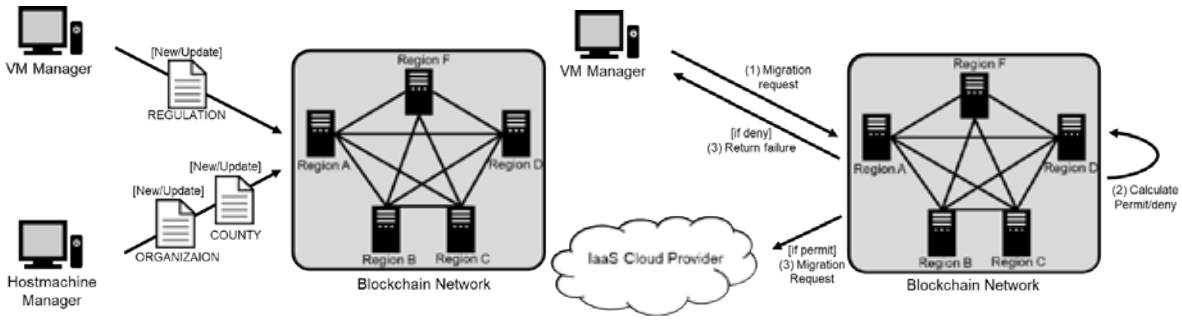
これらの課題を解決するために、点呼者向けと運行管理者向けの 2 種類の従業員管理支援アプリケーションの試作を行った。今後は、サーバのセキュリティ強化とともにプライバシー情報の遵守

を徹底したバックエンド環境の開発を行っていく。さらに、実際の地域公共交通に事業者に本システムを使用して頂くことで評価を行う予定である。

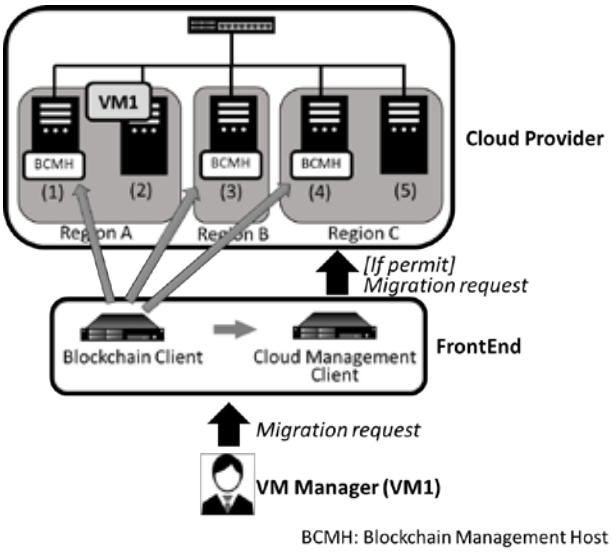
IoT が普及したことで、個人に紐づいた環境を測定する各種センサや個人の健康状態を測定するセンサからの膨大な量のデータをエッジ経由でクラウドへ保管することが一般的となった。IoT で収集されたこれらの膨大な量のデータは、個々の値だけでなく、複数のデータを組み合わせることで、個人の嗜好や行動の予測、行動への介入等に有用な手段を明らかにするため解析がサービス提供者により行われている。これらのデータは個人に密接なデータであり、管理に細心の注意が必要となる。データの所有者の許諾した条件だけでなく、GDPR を代表とする国や地域の法規制、組織の規約を遵守した適切な管理と利用が不可欠である。また、IoT だけでなく、ネットワークを介するアプリケーションやサービスを運用するにあたり、エッジやクラウド環境を利用したサービスが一般的になっており、エッジやクラウド環境なしでの運用は考えられないほど世の中に浸透している。エッジやクラウド環境では、実質的にはコンテナや仮想マシンの中でアプリケーションが動いており、これらのコンテナや仮想マシンは容易に配置や移動（マイグレーション）を行えてしまう。そこで問題となるのが悪意を持った、または無意識に行われる不適切なデータの移動である。そこで、仮想マシンのマイグレーション制御とコンテナのマイグレーション制御に関する研究を行なった。

仮想マシンのマイグレーション制御

仮想マシンのマイグレーション時に、データの所有者の許諾した条件や国の法規制・組織の規約を確実に遵守するための機構を提案する。提案した仕組みをブロックチェーン内に構築することで、悪意のある改ざんを防ぎ堅牢な仮想マシンのマイグレーション制御を可能とする機構を提案した【図 3】。本機構は、マイグレーションのプロセスを変更することなく、さまざまな種類のクラウド環境に適用することができる。実装環境の構成を【図 4】に示す。データ保護機構は、「VM 管理者」、「フロントエンド」、「クラウドプロバイダ」で構成する。「クラウドプロバイダ」は 3 つのリージョンを持つ 5 台のホストマシンで構成される。HostMachine01 と HostMachine03 と HostMachine04 には BCMH(Block-chain Management Host) が設置され、ブロックチェーンにおけるノードの役割を兼任する。また、HostMachine02 には VM1 が稼働している。「フロントエンド」は、クラウド環境内のブロックチェーンへの操作とクラウド環境への操作を行う。マイグレーション実行要求は「VM 管理者」が「クラウドプロバイダ」へ直接行うのではなく、フロントエンドへマイグレーション要求を行う。「フロントエンド」はブロックチェーンクライアントとクラウドマネージメントクライアントで構成される。ブロックチェーンクライアントは、クラウドプロバイダ内の BCMH とブロックチェーンネットワークを形成している。クラウドマネージメントクライアントは、クラウドプロバイダの SDK を操作でき、クラウドプロバイダへマイグレーションの要求を行う。具体的には、OpenStack API を操作するために使用する。提案した機構をブロックチェーン内に構築することで、無意識による不適切なデータの移動や悪意のある改ざんを防ぎ堅牢な仮想マシンのマイグレーション制御を可能とする。提案した機構を既存のプライベートクラウド環境へブロックチェーンとともに実装した。仮想マシンとホストマシンに関するポリシーをブロックチェーンに登録し、ポリシーに準拠した仮想マシンのライブマイグレーションの可否が正確に行われているかを評価し、正しく機能していることを確認した。また、提案した仕組みを利用したライブマイグレーションの実行時間を計測し、本機構を追加したことによる実行時間に差がほぼないことを確認した。



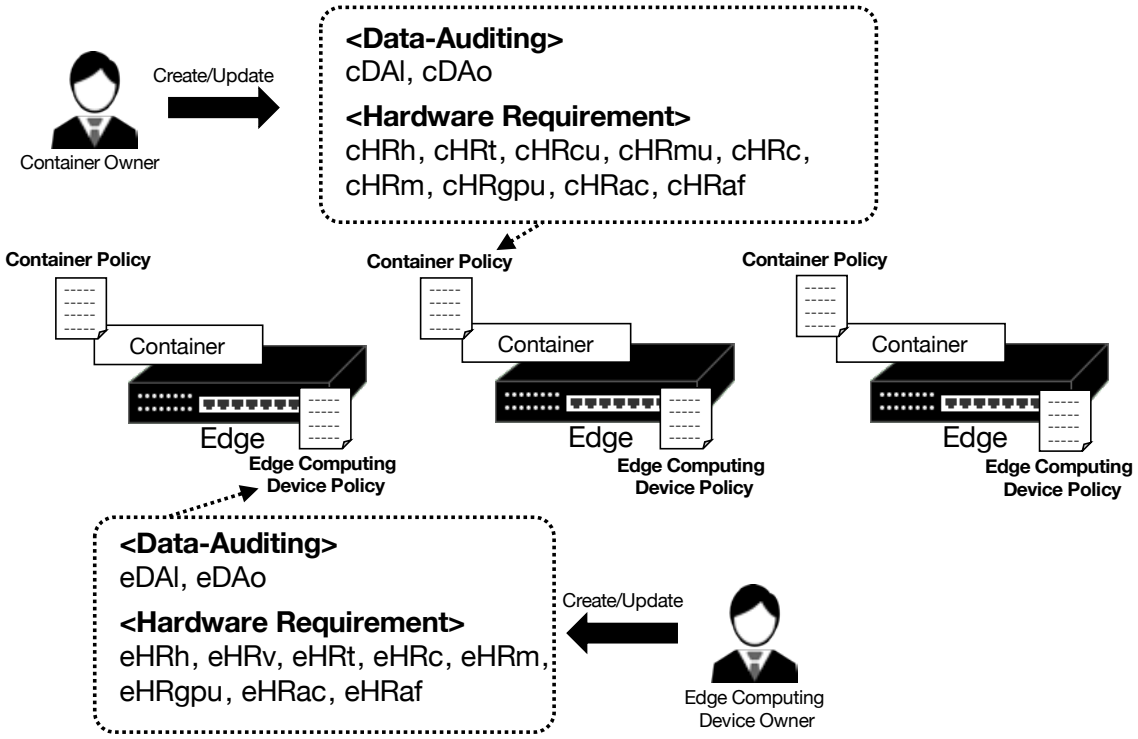
【図 3】　ブロックチェーンを利用したポリシー管理とマイグレーションの可否判定



【図 4】　提案した制御機構の実装

コンテナのマイグレーション制御

仮想マシンのデータ監査機構のポリシーを拡張し、コンテナを対象としたマイグレーション時のデータ監査機構とそのポリシーの提案を行う。仮想マシンのホストマシンとは違いエッジには潤沢な資源はないため、組織や国といった情報に加えてハードウェア要件が必要となる。そこで我々の提案する機構は、組織や国などのデータ監査要件に加えて、ハードウェア要件を追加した。データ監査は、データの移動をソフトウェア的に移動してよいかのチェックを行う。ハードウェア要件は、データの移動をハードウェア的に行ってよいかチェックする。これらのポリシーはコンテナ内とエッジで保管される。コンテナ内では、コンテナの管理者がコンテナ内のアプリケーションやデータの規約に基づいて記述し保管する。エッジでは、エッジの管理者がエッジに準じる情報を記述し保管する【図 5】。これらの記述されたポリシーは基本的に変更されることがないものとする。コンテナのマイグレーション時には、マイグレーションの可否を判断するために、移動するコンテナ内のポリシーと移動先のエッジのポリシーを比較する。移動先のエッジがコンテナ内のポリシーの要件を満たす場合、マイグレーションが実行されるものとする。提案した機構をエッジ環境へ実装した。ポリシーをコンテナとエッジに登録し、マイグレーションの可否が正確に行われているかを評価し、正しく機能していることを確認した。また、提案した仕組みを利用したマイグレーションの実行時間を計測し、本機構を追加したことによる実行時間に差がほぼないことを確認した。

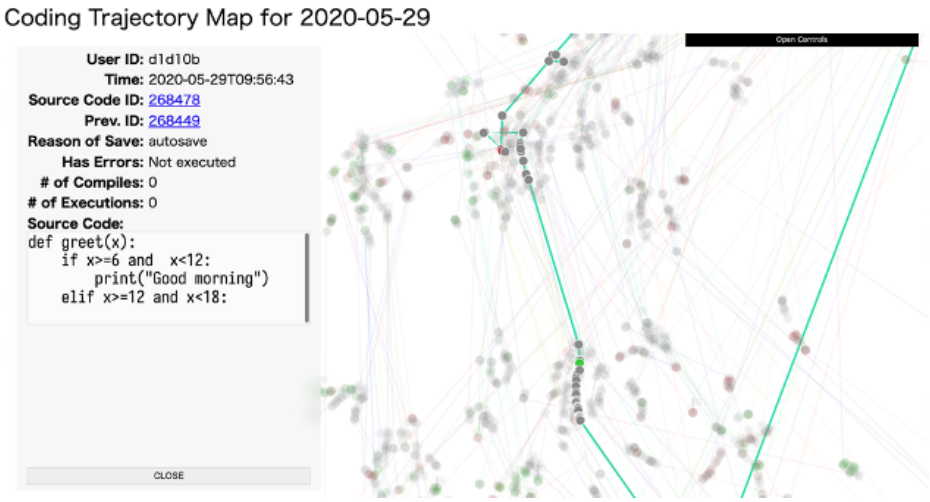


【図 5】　提案した制御機構の実装

7.3　谷口　雄太　〈教育情報基盤研究部門 准教授〉

学生のコーディング過程理解のためのプログラミング演習の軌跡可視化

今日ではプログラミングは重要なスキルの 1 つとされ、小中学校でのプログラミング教育も始まり、また多くの大学では理系の学生だけでなく文系の学生にもプログラミング演習授業が提供されている。プログラミング学習を成功させる上で学習意欲の高さは重要な要因とされているが、多くの学生はプログラムを書くのに悪戦苦闘しており、適切に支援を行わなければ学習者の意欲が低下し、最終的には授業からの脱落に繋がる恐れがある。



プログラミング演習中の学生を支援するためには、学生の学習行動を把握することが重要である。しかし、学生が書いているソースコードを教師が常に確認し続けることは不可能であり、プログラミング教育における大きな困難の 1 つとなっている。本研究は、学生のコーディングプロセスに関して有益な情報を教師に提供することを目的として、高頻度のソースコードスナップショットデータに基づく 2 つの教師向けの可視化フィードバックツールを提案した。

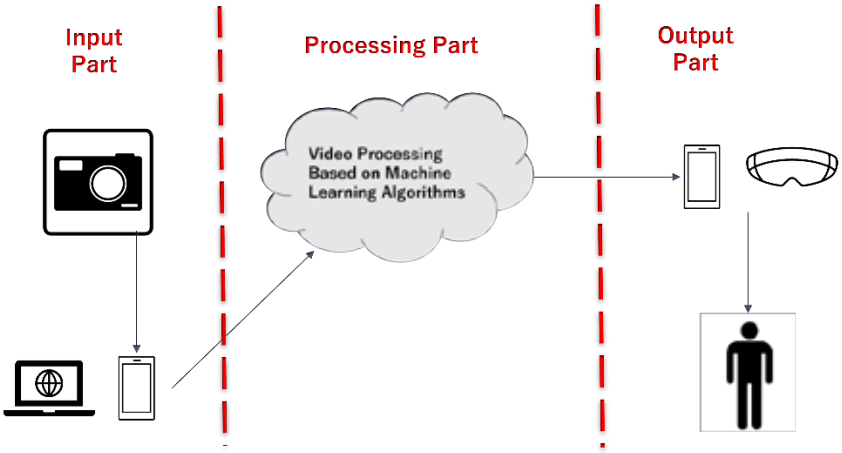
大きく 2 種類の可視化があり、1 つはソースコードレベルでの可視化を提供する。この可視化では、教師はクラス全体の演習の進展具合を視覚的に確認することができる。書いているソースコードの類似性に基づいて、学生の演習状況が 2 次元空間上に配置されるため、同じように演習を進めている学生群と、そうでない学生を視覚的に識別することができる。またもう 1 つの可視化では、ソースコードのクラスタリングを行って、より粗視化された状況を提示する。これにより、演習のパターンを視覚的に類型化する支援を行うことができると考えられる。

プログラミング演習担当教員による評価実験を行った結果、これらのツールは、教師が学生の学習状況をよりよく理解するために有用な情報を提供することが示された。両方の可視化手法は互いに補完的な手法として評価されており、両方をうまく組み合わせることで、より効果的に支援を行うことができる可能性が示された。

7.4　石　偉　〈教育情報基盤研究部門 助教〉

近年、遠隔教育は急速な発展と普及に伴い、電子教材も益々重要になっている。特にスマートフォンなどのモバイルデバイスや、AR・VR デバイスの性能を進化と安価化している共に、ICT 活用した電子教材も注目されている。私は ICT 活用した電子教材の開発に関する研究を行っている。３D・VR･AR 教材を簡単に開発できるフレームワークを提案し、実際に使える電子教材の開発と評価も行っている。2022 年度、日本史、医学、音楽教育分野の先生と連携し、様々な教材の開発を行った。今後、教材の使用状況をモニタリングし、電子教材および教材開発フレームワークの評価する予定である。

他に、私は機械学習の発展と応用も注目している。Computer Vision 技術に基づき、目が不自由の方のための道案内システムに関する研究も同時に行っている。このシステムは３６０度カメラで使用者の周囲環境を録画し、周囲環境をリアルタイムの画像分析を行う。分析結果に基づき、使用者の安全を確保する上に、道案内を行う。【図 1】



【図１】目が不自由の方のための道案内システムの概要

2022 年度には FairMot を実装した歩行者回避システムのプロタイプを開発し、システムの実用性などを検討していた。このプロタイプは使用者の周囲の歩行者を検知し、色と音で使用者へフィードバックする。使用者はこのフィードバックを従うと、他の歩行者との衝突を回避する事が実現できる。【図 2】この研究の成果を国際会議 IIAI-AAI2002 と EIDWT2023 で発表した。[1][2]

【図２】FairMot を利用し、構築したプロタイプで歩行者検知実験

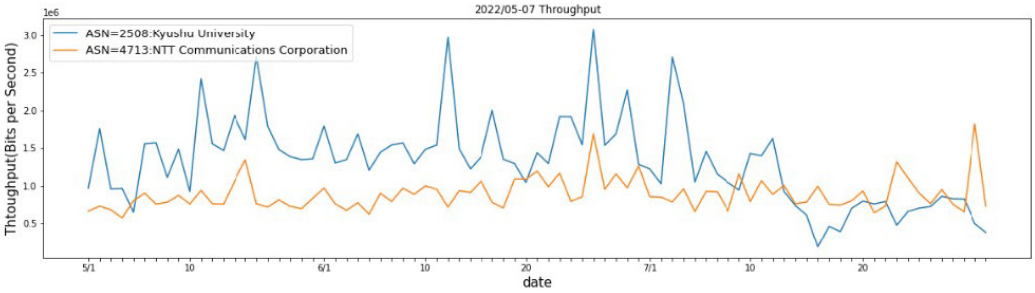
[1] Shi, W., Shan, R., & Okada, Y. (2022). A Navigation System for Visual Impaired People Based on Object Detection. In T. Matsuo, K. Takamatsu, & Y. Ono (Eds.), Proceedings - 2022 12th International Congress on Advanced Applied Informatics, IIAI-AAI 2022 (pp. 354-358). (Proceedings - 2022 12th International Congress on Advanced Applied Informatics, IIAI-AAI 2022). Institute of Electrical and Electronics Engineers Inc..

[2] Shan, R., Shi, W., Teng, Z., & Okada, Y. (2023). A Pedestrian Avoidance System for Visual Impaired People Based on Object Tracking Algorithm. In Lecture Notes on Data Engineering and Communications Technologies (pp. 375-385). (Lecture Notes on Data Engineering and Communications Technologies; Vol. 161). Springer Science and Business Media Deutschland GmbH.

7.5　岡村　耕二　〈先端サイバーネットワーク研究部門 教授〉

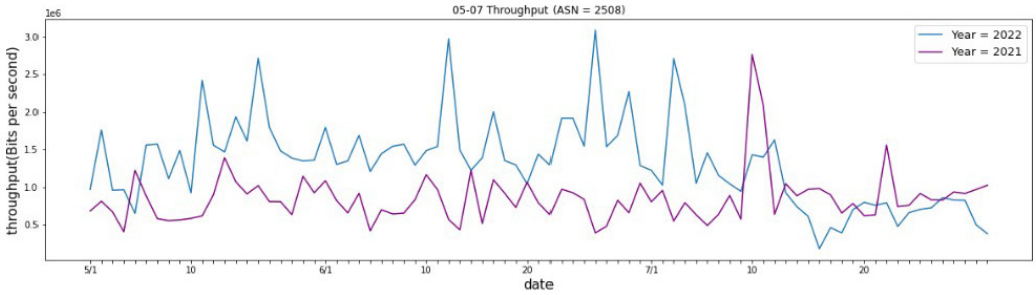
ネットワーク距離とスループットの相関に着目した通信データの解析と考察

TCP 通信のスループットは通信の遅延時間の影響を受け、遅延時間の大きさは通信距離から想定することができる。九州大学では主に、2021 年度はオンラインで、2022 年度は対面で授業が行われたが、この二年の間で九州大学で全学的な LMS (Learning Management System) である moodle の負荷には差が生じていた。そこで本研究では、九州大学のサーバで行われた通信データを解析し、通信のネットワーク距離とスループットの関係について研究した。解析手法として、2021 年と 2022 年の通信、遅延時間や通信距離に差がある通信など複数の視点から計測したスループットの傾向を比較した。



【図 1】学内と学外のスループット

【図 1】は 2022 年の九大内からと　OCN からの Moodle アクセスのスループットを示しており、遅延時間が小さい、通信距離が短い通信のほうがスループットの値は大きくなりやすいということがわかった。



【図 2】2021 年と 2022 年のスループット

【図 2】に示すよう、年度別でデータを比較すると、どの通信も基本的に 2022 年のほうがスループットは大きい値で推移していたことがわかった。スループットが大きいほどサーバでのデータ処理量が多くなるため、レスポンスに要する時間が長くなる。したがって、授業形態の違いによる通信距離の差から 2021 年と 2022 年の間でスループットの大きさに差が生まれ、これにより moodle の負荷に差が生じたと考えられる [1]

参考文献

[1] 小川 智也 , ネットワーク距離とスループットの相関に関する研究 , 九州大学　工学部電気情報工学科 卒業論文

7.6　笠原　義晃 〈先端サイバーネットワーク研究部門 助教〉

End of Basic Authentication and Migration to Modern Authentication for Exchange Online　(Exchange Online サービスにおける基本認証の終了と先進認証への移行について)

Introduction

At Kyushu University, Information Infrastructure Initiative provides email service for all students and staff members, namely “Primary Mail Service” with Microsoft 365 Exchange Online[1]. In Sep. 2019, Microsoft announced its plan to end the support of Basic Authentication for email protocols (including POP3, IMAP4, and SMTP) in Exchange Online, which would significantly impact our user population using email applications. Microsoft’s original plan was to retire Basic Authentication on Oct. 13th, 2020, but it was postponed due to the COVID-19 outbreak.

In Sep. 2021, Microsoft announced a resumption of its plan and set the end of Sep. 2022 as the hard deadline for disabling Basic Authentication. In this section, we share our experiences about the effect of retiring Basic Authentication for Exchange Online on our service and users.

Basic Authentication

Basic Authentication means an application sends a username and password (often stored on the device) directly to the service. Once user credentials leak via phishing, eavesdropping, or malware infection, email protocols are vulnerable to illegal access because of their trivial authentication mechanism. Also, it is hard to implement additional protections such as MFA due to its simplicity. Microsoft strongly encourages customers to move away from using Basic authentication.

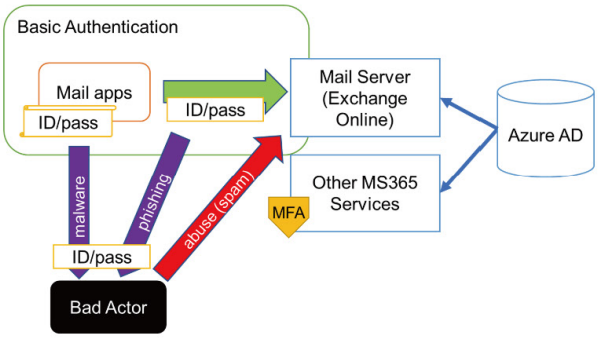


Figure1　Basic Authentication for Email Service

Modern Authentication for Email Service

In 2010, Yahoo and Google extended email protocols to support the OAuth mechanism[2][3]. It was standardized as RFC7628[4]. Microsoft supported Modern Authentication for their proprietary MAPI protocol in 2015. To support Modern Authentication, the email application must be modified to support HTTP, direct users to a token endpoint, authenticate themselves, and receive an access token. The token is used for authentication and is only valid for email services.

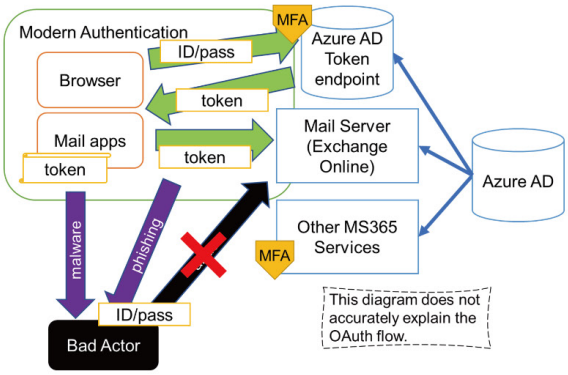


Figure 2　Modern Authentication for Email Service

Before the Deprecation

Historically, our email app users mostly used IMAP/POP/SMTP instead of MAPI (Exchange). In 2019, Exchange Online only supported Modern Authentication for MAPI. We had to wait until more information was available to plan our migration. Microsoft implemented OAuth 2.0 for IMAP, POP, and SMTP in April 2020. We started researching how to use Modern Authentication with various email apps. In Sep. 2021, Microsoft announced its new plan to deprecate Basic Authentication at the end of Sep. 2022 (one year ahead) but also told to disable it for a short period randomly from Jan. 2022 (in four months!). We scrambled to prepare detailed migration manuals and announced to all users about the migration on Nov. 18th, 2021. In Jan. 2022, we blocked Basic Authentication for new users. Due to the limitation of Azure AD, we had to make a custom Power Automate flow to collect Basic Authentication usage reports (the graph below). Still, data were incomplete due to various limitations. The graph shows that we nudged the remaining users several times, but the effect was limited. We blocked Basic Authentication on Oct 1st, 2022.

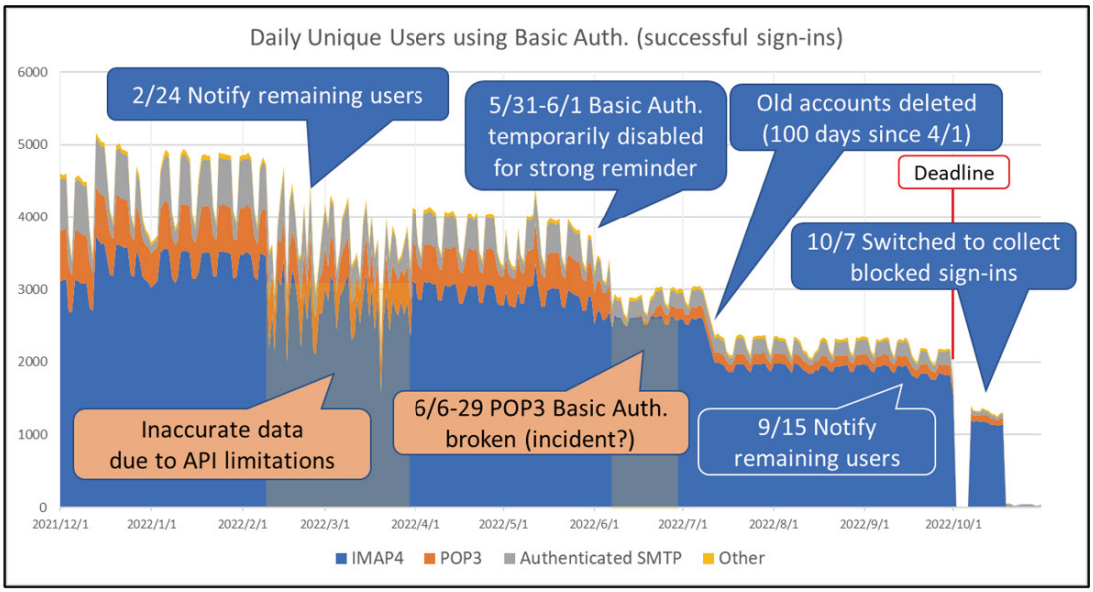


Figure 3　Basic Authentication Usage Trend and Related Events

After the Deprecation

After each notification, we received inquiries from our users, but the number was less than anticipated (a few dozen, but less than a hundred). Even after we blocked Basic Authentication completely, these inquiries calmed down after two weeks. The remaining sign-in failures seemed to be abandoned, and it was good to block such accesses to reduce the risk of abuse. On Oct. 18th, 2022, Microsoft support changed our tenant setting to block Basic Authentication entirely. Attempts of Basic Authentication would be blocked before authentication, and we couldn't see sign-in logs with Basic Authentication anymore. Authentication requests to our on-premise ADFS were significantly reduced (about 1/20) because Modern Authentication was handled mainly by Azure AD. Thanks to Modern Authentication, We'll fully leverage the power of Azure AD MFA, Conditional Access, and Identity Protection for email service.

References

[1] Yoshiaki Kasahara, Takao Shimayoshi, Tadayuki Miyaguchi, and Naomi Fujimura. 2019. Migrate Legacy Email Services in Kyushu University to Exchange Online. Proc. SIGUCCS '19, ACM, 127–131. https://doi.org/10.1145/3347709.3347817

[2] Dick Hardt. 2012. The OAuth 2.0 Authorization Framework. RFC 6749. https://doi.org/10.17487/RFC6749

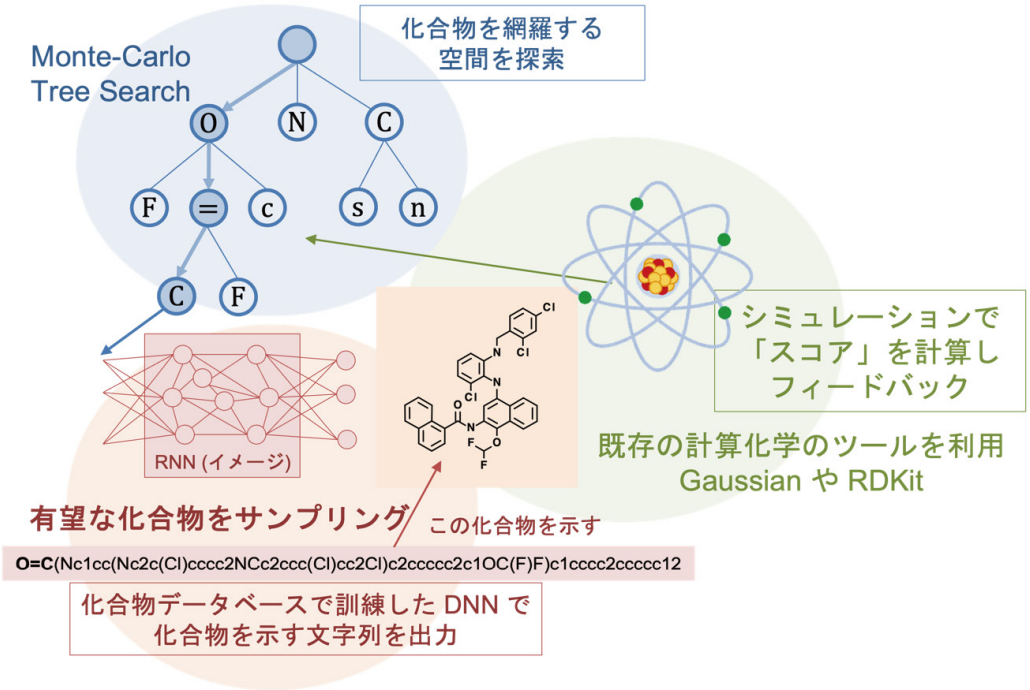
[3] Michael Jones and Dick Hardt. 2012. The OAuth 2.0 Authorization Framework: Bearer Token Usage. RFC 6750. https://doi.org/10.17487/RFC6750

[4] William Mills, Tim Showalter, and Hannes Tschofenig. 2015. A Set of Simple Authentication and Security Layer (SASL) Mechanisms for OAuth. RFC 7628. https://doi.org/10.17487/RFC7628

7.7　美添　一樹　〈先端計算科学研究部門 教授〉

昨年度まで、機械学習と探索アルゴリズムを大規模並列で動作させて化合物探索に応用する研究に取り組んでいた。これは AlphaGo も用いていたモンテカルロ木探索に、RNN を用いた化合物文字列のサンプリングと第一原理計算によるシミュレーションを組み合わせて、化合物を評価しながら探索するアルゴリズムによる。さらにこの研究成果にもとづくソフトウェアを公開している。

2022 年度はこのソフトウェアの普及のため、化合物のスコアを利用者が自由に定義できる仕組みを提供した。また性能向上やインストール手順を容易にするなどの実装の改良も行った。現在はアルゴリズムのさらなる性能向上や応用範囲の拡大を目指して研究を継続している。



参考文献

Shoichi Ishida, Tanuj Aasawat, Masato Sumita, Michio Katouda, Tatsuya Yoshizawa, Kazuki Yoshizoe, Koji Tsuda, Kei Terayama, ChemTSv2: Democratizing Functional Molecular Design Using de novo Molecule Generator, ChemRxiv, 2023 年 2 月 .

7.8　渡部　善隆　〈先端計算科学研究部門 准教授〉

ヒルベルト空間における線形作用素の可逆性理論の構築

非線形関数方程式の解の存在を無限次元ニュートン法の枠組みにおいて厳密な誤差評価付きで検証するためには、適切な方法で得られた離散近似解において非線形問題を線形化して得られる線形化作用素の可逆性の検証、および、具体的な逆作用素ノルムの評価が重要な役割を果たすことが知られている。

2021 年度までの研究において、2 階楕円型線形作用素の可逆性の理論的な保証と数学的に厳密な意味での逆作用素ノルムの上界を精度保証付き数値計算によって求める手法の開発を行った。これは、楕円型作用素を理論的・数値的な知見が得られている 2 階微分作用素項と 1 階微分以下の摂動項に分離し、摂動項に対応する作用素と有限次元部分空間の基底との内積で構成される行列を用いることにより、可逆性の検証と逆作用素ノルム評価を分けて考えるアイデアに基づくものである。この手法を具体的な問題に対して適用した結果、可逆性の検証および逆作用素の上界の評価ともに、既存の手法に比較して大幅な改善となることを理論面・応用面から明らかにした。2022 年度は、得られた理論と技術を一般のヒルベルト空間（内積から導かれるノルムがバナッハ空間となる関数空間）における線形作用素に拡張することに取り組んだ。

2 階楕円型線形作用素に対する基本的なアイデアを踏襲し、理論的・数値的な知見が得られている主要項とそれ以外の摂動項に線形作用素を分離し、摂動項に対応する作用素と有限次元部分空間の基底との内積で構成される行列が妥当な仮定の下に作成可能であることを示した。一般のヒルベルト空間における線形作用素の可逆性の検証と逆作用素ノルム評価に関する先行研究としては、不動点定式化に基づく方法と、直接ノルム評価を行う 2 つの方法が提案されていた。これらの先行研究はそれぞれにおいて特長を有する優れた成果ではあるものの、個々の問題に応じて適用範囲に制限があった。今回拡張・応用を行った手法は、無限次元作用素の摂動項を効率的に見積もるノルム評価を経由する新しい方法論であり、2 つの既存手法の特長を包含する形で、かつ、同等の計算量で効率的に可逆性の検証と逆作用素ノルム評価が達成可能であることを具体例により明らかにした。この成果を様々な非線形関数方程式に応用することにより、今後、検証可能な問題の適用範囲が格段に広がることが期待できる。研究成果は 2022 年度内に学術論文として掲載された。

▶ Yoshitaka Watanabe, Takehiko Kinoshita, and Mitsuhiro T. Nakao:
Efficient approaches for verifying the existence and bound of inverse of linear operators in Hilbert spaces, Journal of Scientific Computing, vol. 94, Article number: 43 (January 2023).
https://doi.org/10.1007/s10915-023-02097-6

掲載雑誌は、応用数学分野でインパクトファクター上位 15% 以内に入る著名な国際学術誌である。検証においては、九州大学情報基盤研究開発センターのスーパーコンピュータシステム ITO を活用した。

共同研究

2022 年度に行なった共同研究は以下の通りである。

1. 無限次元線形化作用素の可逆性判定とノルム評価の効率化
   共同研究者 : 中尾 充宏（早稲田大学）木下 武彦 (佐賀大学)
2. 非線形波動方程式に対する計算機援用証明
   共同研究者 : Michael Plum, 長藤 かおり（ドイツ・Karlsruhe 工科大学）
3. Navier-Stokes 方程式に対する計算機援用安定性解析
   共同研究者 : Shuting Cai (中国・Fujian Jiangxia 大学)
4. Proudman-Johnson 方程式の解の検証および解の形状に関する精度保証付き数値計算
   共同研究者 : 宮路 智行 (京都大学)
5. Kolmogorov 問題から導かれる最大値ノルム評価の改良
   共同研究者 : 小林 健太 (一橋大学)

7.9　南里　豪志〈先端計算科学研究部門 准教授〉

NVDIMM 上の時系列バッファ実装による効率的な非同期連成計算の実現

研究の背景

近年、DRAM と同様に DIMM スロットに搭載できる NVDIMM と呼ばれる不揮発性メモリが普及しつつある。これは DRAM に準ずる数百ナノ秒のアクセス遅延と SSD に近い価格対容量を兼ね備えた新しい記憶装置であり、計算科学やデータ科学の様々な分野で、性能と容量の制約により解決が難しかった問題に取り組むための手段として注目されている。

本研究では、この NVDIMM を非同期連成計算のための時系列バッファに応用する。連成計算とは、異なる事象を組み合わせた複雑な問題を解くために新しい一つのプログラムを作る代わりに、各事象を解く既存のプログラムを連結させ、相互に情報を交換しながら計算させる、というものである。これによりプログラム開発コストを大幅に軽減できるため、これまで困難だった様々な問題に効率よく取り組むことができる。例えば代表者らは、この連成計算を簡潔に実現するためのフレームワーク CoToCoA を開発し、さらに宇宙プラズマの微視的現象と巨視的現象を組み合わせた問題にこのフレームワークを適用して実用性を検証してきた。

このような連成計算において、計算効率面で大きな問題になるのがプログラム間の同期待ちである。連成計算は、あるプログラムが生成したデータを他のプログラムが参照するという依存関係で成り立っている。そのため、CoToCoA を含む従来の連成計算では、プログラム間で時間ステップごとに待ち合せながら計算を進める同期的な手法が用いられていた。また、各プログラムのステップごとの計算量からそれぞれに割り当てる CPU コア数等の計算資源量を調整することで、この同期待ちに要する時間の削減が図られてきた。しかし多くのプログラムでは、データの内容や計算の進捗に応じた計算量の変化等により計算速度が変動する。また、片方のプログラムで発生したイベントに応じてもう片方のプログラムによる解析を開始するイベント駆動型の連成計算も存在する。このような非同期性のため、多くの連成計算では同期待ち時間が増大し、その結果、待たされる側のプログラムが使用する計算資源を無駄に休ませることになっていた。

これに対し、データの生成側と参照側のプログラム間に、時系列でデータを保管できるバッファ領域を用意すれば、プログラム間の明示的な同期が不要な、非同期連成計算を実現できる。しかし、このバッファ領域を DRAM 上に置くとプログラムが利用可能なメモリ空間を圧迫し、SSD や HDD 上に置くとアクセス遅延時間のため連成計算の性能が大幅に低下する。そのため、いずれも実用的な実装が困難であった。これに対し、低遅延大容量の NVDIMM 上にこのバッファを配置することで、これらの制約を解消し、効率的で実用的な非同期連成計算の実現が期待できる。

今年度の実績

まず非同期連成計算用時系列バッファ領域のインタフェース設計に取り組んだ。非同期連成計算では、あるプログラムがバージョン毎に生成するデータを、別のプログラムが適宜参照する。そこで、データごとに生成側のプログラムを生産者、参照側のプログラムを消費者として登録し、役割に応じて操作する、生産者消費者モデルのインタフェースを設計した。生産者の基本操作は新規バージョンの追加のみとし、既存バージョンの書き換えを不可とする。この方針に基づき、生産プログラム側からバージョン番号と生成データをバッファに入力する関数、および、参照側から任意のバージョンのデータと取得する関数を設計した。さらに、バッファに空きを作るため、不要になったバージョ

ンを削除する関数、およびデータをファイルに移動する関数も設計した。

次にこれらの実装に取り組んだ。バッファへの入力関数は、バッファに空きがあれば即座にデータをコピーして終了し、空きが無ければ、参照側の操作で空きが生じるまで待つようにした。これらの動作を確認したところ、参照側のデータ取得の際のオーバヘッドが大きいことが判明した。そこで、一度のデータ取得で周辺のバージョンのデータも取得するキャッシュ機構を追加実装することで、オーバヘッドの低減を実現した。

また、プログラミングインタフェースとしての実用性を確認するため、共同研究者の加藤、深沢、三宅らが開発している磁気流体シミュレーションプログラムとその可視化プログラムを利用して、連成計算の一つである In-situ 可視化を実現し、問題なく利用できることを検証した。

なお、本年度購入予定だった NVDIMM については、開発元の Intel 社が開発を停止したため、1 年前に購入していた製品で代用することとした。一方、NVIDIA 社の最新のネットワークカード BlueField2 を購入することで通信時間を短縮し、実用性の向上を図った。

今後の方針

時系列バッファ領域の NVDIMM への実装に取り組む。NVDIMM 上に時系列バッファ領域を構築し、各インタフェースを実装する。実装環境は、既存クラスタ環境の NVDIMM と InfiniBand NIC を最新の製品に更新して使用する。データの生成、参照時の通信手段は全て RDMA を用いる。RDMA は非同期で非ブロッキングの通信が可能であるため、非同期連成計算を低オーバヘッドで実装するために必要である。また、NVDIMM 領域が不足した場合の動作として、初年度に設計したバージョンの削除やファイルへの移動インタフェースを応用し、生産者、消費者の進捗状況に応じて、特定のバージョンの退避や削除、さらに、NVDIMM に空きが出来るまで生産者からのバージョン追加要請の処理を待つ、のいずれかを自動選択する機構を実装する。この機構の動作条件等の調整において、加藤、深沢、三宅による利用者視点での意見を取り入れる。

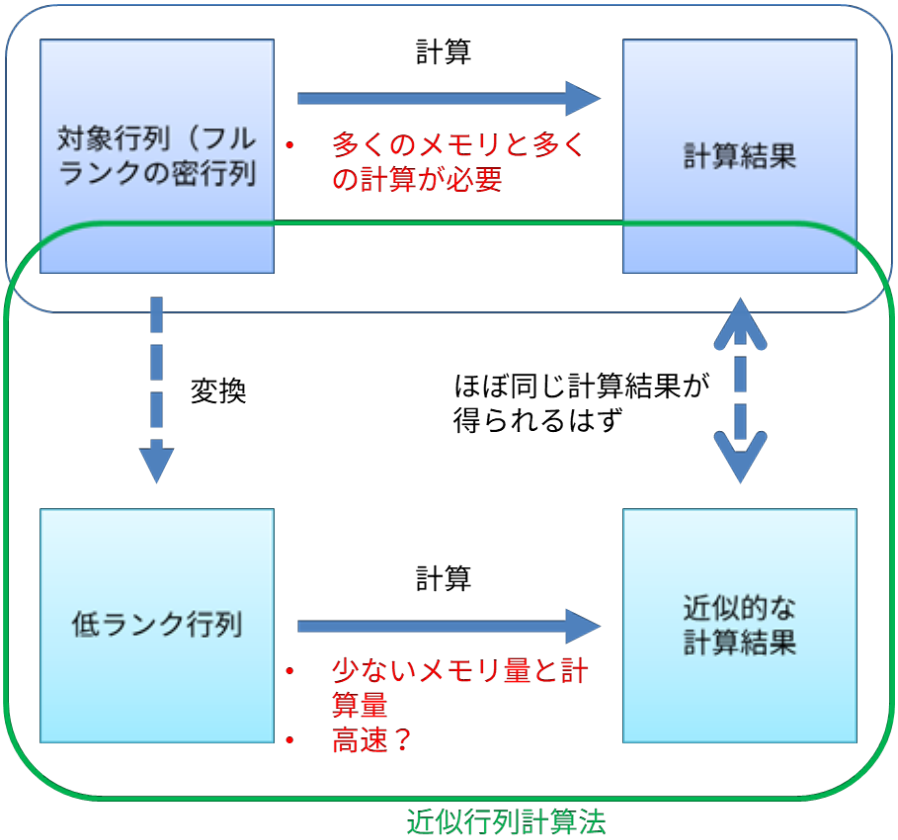
その後、時系列バッファ領域を利用した非同期連成計算の実現と評価に取り組む。開発した時系列バッファを利用し、加藤が開発した電磁圏内の高エネルギー粒子環境をミクロ計算で解くプログラムと、深沢が開発した太陽風の変動に伴う磁気圏構造の変化を磁気流体力学 (MHD) で解くプログラムの非同期連成を実現する。さらに、三宅が開発した人工衛星帯電予測プログラムとの非同期連成についても取り組む。その後、時系列バッファのオーバヘッド計測や同期と非同期での連成計算の効率比較を通じて、実用性を検証する。

7.10　大島　聡史　〈先端計算科学研究部門 准教授〉

GPU を用いた BLR 行列に対する QR 分解に関する研究

研究の背景

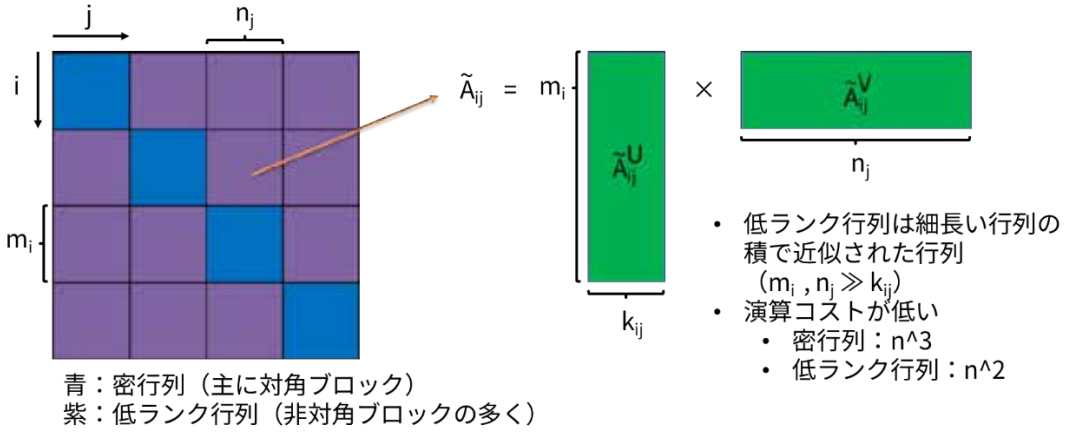
大規模な計算や複雑な計算を高速に行いたい、そのために大規模な密行列を扱う計算を行いたいという需要は大きい。しかし大規模な密行列計算は多くの計算量と大きな記憶容量を必要とするのに対し、近年の計算ハードウェアは演算性能の向上に比べてメモリの速度や容量の向上が追いついていないのが現状である。そこで、密行列を近似して扱うことでメモリ性能への負荷を減らす近似行列計算法が注目されている。近似行列計算法では対象となる密行列に対して低ランク化を行い、低ランク化された行列に対して演算を行い、元の密行列に対して演算を行ったのと近い計算結果を低コスト（高速、省メモリ）に得ることを目指す【図 1】。そのためには低ランク化手法と低ランク行列に対する計算法の両方が重要である。



【図 1】近似行列計算法の概要

近似行列計算法で用いられる行列近似法（近似行列形式）にも様々なものがあるが、本研究ではブロック低ランク（Block Row Rank、BLR）行列 [参考文献 1] を用いる【図 2】。BLR 行列はブロック化した行列の一部を低ランク化した行列である。低ランク化は対象問題の物理的な意味を元に行われ、例えば近い距離の相互作用と比べて遠い距離の相互作用は影響が小さいため、前者を密行列、

後者を低ランク行列として扱うといった具合である。BLR 行列では一般的に、行列の対角付近のブロックは密行列であり、低ランク行列となるのは非対角ブロックが主である。BLR 行列は構造が単純であるため、他の低ランク近似行列と比べて必要なメモリ容量は大きくなりがちであるが、計算を行いやすく、並列計算時の負荷バランスの調整もしやすい。



【図 2】BLR 行列

本研究では BLR 行列に対する QR 分解（BLR-QR）の高速化を目指している。QR 分解は様々な科学技術計算や数値計算にて用いられる基本的な問題であり、大規模な行列を高速に QR 分解したいという需要は大きい。CPU クラスタにおける BLR-QR についてはすでに参考文献 2 にて共同研究者らが取り組んでおり、本研究ではさらなる高性能化を目指して GPU を用いた BLR-QR の高速化に取り組んでいる。以下、発表論文等 1 にて発表した内容を元に本研究の内容を紹介する。

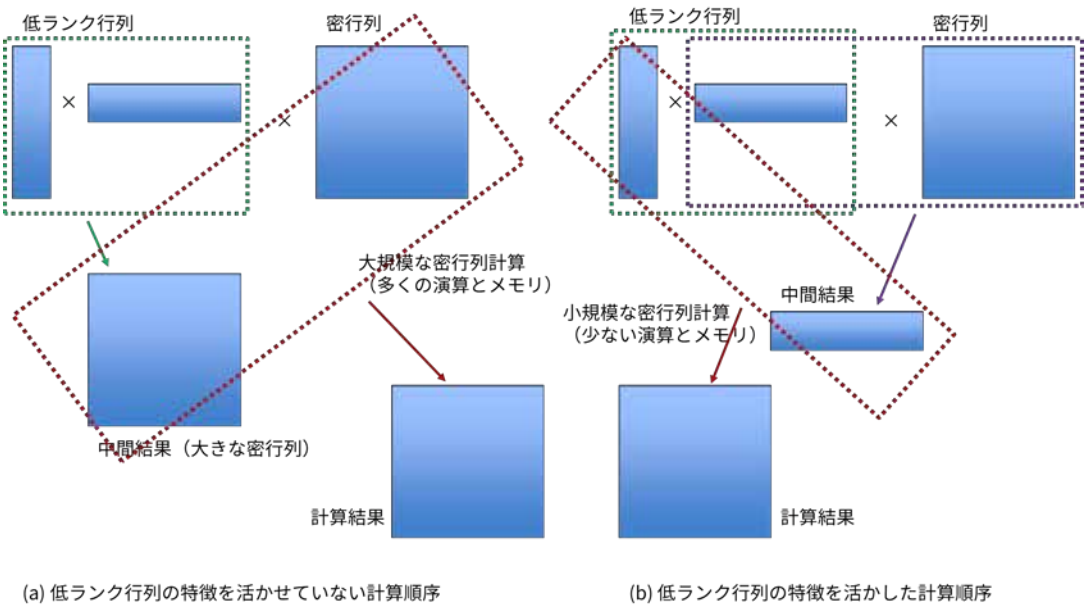
実装

本研究では参考文献 2 における CPU クラスタ向けの実装（以下、既実装）を元に GPU 向けの実装を行った。

既実装は Fortran90 で記述されており、MPI と OpenMP を用いて並列化されている。QR 分解アルゴリズムとしては修正ブロックグラムシュミット（Modified Block Gram Schmidt, MBGS）法【アルゴリズム 1】が用いられている。BLR 行列に対しても MBGS 法が適用可能であり、基本的にブロック化された密行列に対する QR 分解と同様に QR 分解が可能であるが、ブロックが低ランク化されている場合にはその構造に合わせて計算内容を変更する必要がある。具体的には、例えば密行列積に対する MBGS 法においては密行列ブロックと密行列との積を計算する必要があるが、BLR-QR ではその一部を低ランク行列と密行列の積に変更する必要がある。低ランク行列と密行列の積は、低ランク行列が細長い密行列同士の積により構成されるため、計算順序を工夫する（細長い密行列同士の積を計算してから密行列と掛け合わせるのではなく、細長い密行列と密行列の積を 2 回実行するようにする）ことでメモリ使用量と計算量を減らすことができる【図 3】。また低ランク行列に対する計算を行うと行列のランクが増加してしまうことがあり、増加したランクを減らす低ランク化処理も重要である。

```
Input  : A with N_b × N_b blocks
Output : Q, R with N_b × N_b blocks
         such that QR=A
For  j = 1,2,…,N_b  do
    [Q_{*,j}, R_{j,j}] := TSQR(A_{*,j})
    For  k = j+1, j+2, …, N_b  do
        R_{j,k} := Q^T_{*,j} A_{*,k}
        A_{*,k} := A_{*,k} − Q_{*,j} R_{j,k}
    End do
End do
```

【アルゴリズム 1】修正ブロックグラムシュミット（MBGS）法



【図 3】密行列 - 密行列積と低ランク行列 - 密行列積

既実装においては行列に対する多くの演算を BLAS や LAPACK の提供する関数を用いて実装することで実装の容易さと高性能を達成した。GPU においても cuBLAS や cuSOLVER が対応する関数を提供しているため、これらを用いれば容易に BLR-QR を実装することができる。しかしながら、GPU は多数の計算コアが高い並列度で処理を行うことで高い性能を得るハードウェアであるのに対し、BLR-QR で使う計算は GPU にとって効率良く演算できるほど十分な並列度を有していない。そのため、cuBLAS や cuSOLVER を用いても GPU が高い性能を発揮することは期待できない。各ライブラリの関数が GPU の一部のみを用いて妥当な性能を出すことができる実装であれば、GPU 内で複数の関数を同時に実行して妥当な高性能を得ることもが可能であるが、一般的な GPU 向け計算ライブラリは利用可能な計算資源を最大限に利用して最大性能を得ることを志向するのが自然である。CPU や GPU に搭載された計算コアの数が増加している今日、このような問題は BLR-QR に限らず多

くのアプリケーションで発生している。その対策として、小規模な計算であっても多数同時に実行することで高い並列度の計算を行い全体として高性能を目指すバッチ計算が利用されている。既にMKL ライブラリ、cuBLAS、cuSOLVER など著名な数値計算ライブラリがバッチ計算をサポートしている。しかしバッチ計算を利用するには専用のデータ構造を利用する必要があることが多く、データの再構成や抜本的なデータ構造の見直しなどが必要となる。

そこで本研究では、GPU を分割して利用することができる Multi Instance GPU(MIG) 機能を用いることを提案した。MIG を用いればユーザプログラムからは分割された小さな GPU（サブ GPU）が複数存在するように見えるようになり、cuBLAS などのライブラリの提供する関数も含めて各 GPU カーネルをサブ GPU に閉じ込めることが可能となる。MPI 並列化されたプログラムにて各 MPI プロセスがそれぞれサブ GPU に計算を行われるような設計とすることで全体として高性能な BLR-QR の実現が期待できる。

そこで既実装をもとに、oneAPI MKL ライブラリの関数を呼び出している部分を cuBLAS や cuSOLVER の関数呼び出しに置き換え、その他の行列やベクトルに関する計算も GPU 上で行われるようにプログラムを修正した。既実装は Fortran90 にて実装されていたが、GPU に関する処理は C/C++ および CUDA C で実装して Fortran90 コードから呼び出すようにした。

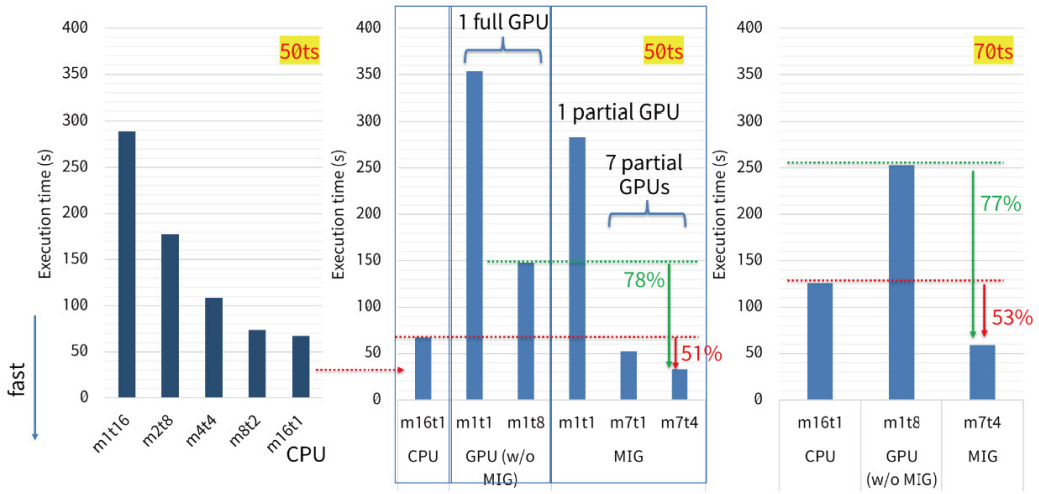
性能評価として、いくつかの行列に対する QR 分解の性能を測定した。測定範囲はアルゴリズム 1 の主要な計算部である 4 行目と 5 行目の総和とした。実験環境としては以下の構成のワークステーションを用いた。

- CPU: AMD EPYC 7313, Milan, 16 コア /32 スレッド（物理コアのみ使用）, 3.0GHz, 768GFlops (FP64)
- メインメモリ : DDR4-3200 512GB, 205GB/s
- GPU: NVIDIA A100 40GB PCIe, Ampere, 9.7TFlops (FP64)
- デバイスメモリ : HBM2 40GB, 1,555GB/s
- コンパイラ : Intel oneAPI Toolkits 2021.5.0, NVIDIA CUDA 11.6.2

対象問題としては境界要素法を用いた静電場解析問題から得られる行列を用いた。行列の諸元を【表 1】に示す。大小 2 つの行列を用いているが、物理的にはいずれも空間に球体が 1 つだけある単純な問題であり、行列の大きさ（一辺の長さ）が異なる。

	密行列の一辺の長さ	ブロックサイズ	7 プロセス実行時の最大ランク	7 プロセス実行時の平均ランク	BLR 行列のメモリ量
50ts	50,864	32*32	273	45	1,777 MB
70ts	69,312	32*32	304	39	2,625 MB

【表 1】対象問題



【図 4】性能評価結果

実行結果を【図 4】に示す。図 4 左図は対象問題 50ts に対して CPU のみを用いた際の実行時間であり、横軸の mAtB 表記は MPI A プロセス、1 プロセスあたり OpenMP B スレッドでの実行を意味する。右の縦棒ほど短くなっており、フラット MPI による実行が一番高速であることがわかる。図 4 中図は対象問題 50ts に対して CPU と GPU の実行時間を比較したものである。MIG を使わない場合の GPU の実行時間は CPU と比べて長いが、MIG を使った場合は最も良いケースで CPU の 51% まで実行時間を短縮できている。図 4 右図は対象問題をより大きな 70ts にした場合の結果で、50ts のときと同様に CPU の 53% まで実行時間を短縮できた。

研究成果

以上に示したように、MIG を用いることで GPU を用いた BLR-QR の性能を大幅に向上させることに成功した。本研究の成果は発表論文等 1 の査読付き国際会議にて発表し、同 2 に掲載された。また、本成果の前段階やその後の課題について発表論文等 [3],[4],[5] にて口頭発表した。

本研究にはいくつかの課題が残っている。まず本研究では GPU に関する処理を C/C++ および CUDA C で記述したが、Fortran90 で記述された既実装コードからこれらを呼び出す実装では CPU-GPU 間のデータ転送をできるだけ少なくするような実装は容易ではない。（不可能ではないが、コードの見通しが悪く難しい。）そのため CUDA Fortran などを用いて実装した方が最適化を行いやすい可能性がある。また、MIG を使った場合の GPU プログラムの難点として 1 サブ GPU あたりの GPU メモリ量が減ってしまうため大きな対象問題を扱いにくい、扱いたければホストメモリとデバイスメモリでデータの入れ替えなどを行わなければならない。これも不可能ではないが、BLR-QR に限らず Fortran90 プログラムを容易に GPU 移植して高い性能を得たいという要求は多く、これに応えられているとは言い難い。ホストメモリとデバイスメモリを統一的に扱うことのできる Unified Virtual Memory (UVM) と組み合わせることでより簡単に高い性能が得られる可能性があり、今後の課題である。最後に、今回は BLR-QR 全体での性能は追求できていないため、全体で高性能を達成することも今後の課題である。

参考文献

[1] Ida, A., Nakashima, H., Kawai, M.: Parallel Hierarchical Matrices with Block Low-rank Representation on Distributed Memory Computer Systems, Proc. International Conference on High Performance Computing in Asia-Pacific Region, pp.232-240, ACM (2018). DOI: 10.1145/3149457.3149477

[2] Ida, A., Nakashima, H., Hiraishi, T., Yamazaki, I., Yokota, R., Iwashita, T.: QR Factorization of Block Low-rank Matrices with Weak Admissibility Condition, Journal of Information Processing, Vol. 27, pp. 831-839 (2019). DOI: 10.2197/ipsjjip.27.831

発表論文等

[1] Satoshi Ohshima, Akihiro Ida, Rio Yokota, Ichitaro Yamazaki, “QR Factorization of Block Low-Rank Matrices on Multi-Instance GPU”, The 23rd International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT’ 22), 2022.12.7-9 開　催、2022.12.8 発表 , pp.1-11

[2] Satoshi Ohshima, Akihiro Ida, Rio Yokota, Ichitaro Yamazaki, “QR Factorization of Block Low-Rank Matrices on Multi-Instance GPU”, Parallel and Distributed Computing, Applications and Technologies, Springer Nature Switzerland, pp.359-369, 2023.04 発行 , DOI:10.1007/978-3-031-29927-8_28

[3] Satoshi Ohshima, “QR Factorization of Block Low-rank Matrices on GPU”, 第 41 回 ASE 研究会 , オンライン , 2022.02.04 開催 , 2022.02.04 発表

[4] Satoshi Ohshima, “QR Factorization of Block Low-rank Matrices on Multi-Instance GPU”, ATAT in HPSC, オンライン , 2022.03.29-30 開催 , 2022.03.30 発表

[5] 大島聡史 , 伊田明弘 , 横田理央 , 山崎市太郎 , “BLR-QR on GPU：マルチインスタンス GPU を用いた多数の小密行列計算の高速化 ”, 第 14 回 自動チューニング技術の現状と応用に関するシンポジウム（ATTA2022）, 工学院大学新宿キャンパス +Zoom, 2022.12.23 開催 , 2022.12.23 発表

[6] Satoshi Ohshima, “QR Factorization of Block Low-rank Matrices on Multiple-/Multi-Instance GPUs”, ATAT in HPSC 2023, 國立中央大學 健雄館 , 2023.03.24-25 開催 , 2023.03.24 発表

7.11　樋口　祐次 〈先端計算科学研究部門 准教授〉

ソフトマターの分子シミュレーション

生体膜の主成分であるリン脂質分子は、水中で自己組織化して二重膜構造を形成する。リン脂質分子は生体適合性が高いことから、ドラッグデリバリーシステム (DDS) などへの応用も進んでいる。生体ではイオン、タンパク質、DNA といった電解質が存在している。電荷をもつ荷電リン脂質の分子集合構造と集合体近傍のイオン分布は、長距離の静電相互作用により互いに相関している。このため、脂質分子の自己組織化プロセスや構造を理解するには、静電相互作用の解明が必須である。

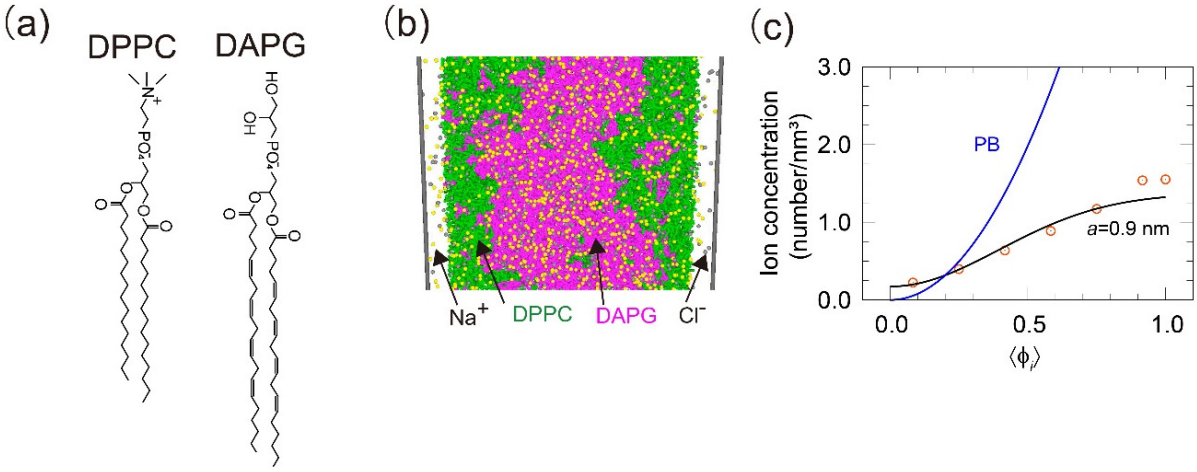
実験において、荷電リン脂質を用いることで、中性脂質では見られない相分離挙動が観察されている。また、低塩濃度において荷電脂質と中性脂質が相分離し、荷電脂質ドメインから空孔が形成され、膜が不安定化しベシクルからディスク状に変形するプロセスも観察されている。これらから、静電相互作用により相分離挙動や安定な膜構造が変化することが示されている。一方で、荷電リン脂質の相分離挙動とイオン分布の関係性に関しては、実験で直接観察することが難しく、明らかになっていない。そこで、粗視化分子動力学シミュレーションを用いて、荷電リン脂質分子が相分離した際の、二重膜直上のイオン分布の解析を行った。

相分離している脂質膜上におけるイオン分布を明らかにするために、GROMACS を用いて分子動力学計算を行った。三次元周期境界条件で、片側 1024 分子から構成される脂質二重膜を、膜間の水層が約 20 nm となるように作成した。塩濃度は NaCl 100 mM において、中性の DPPC 分子と、負電荷をもつ DAPG 分子を 1:1 で混合した。リン脂質分子の構造を図 1 (a) に示す。

粗視化分子動力学シミュレーションを行い、5 μs 経過後のスナップショットを図 1(b) に示す。DPPC と DAPG が別々に集合している相分離状態が観察された。相分離プロセスの経過を見てみると、カチオンは負に帯電したリン脂質分子に追従する様子が観察された。このことから、カチオンと負に帯電した脂質との間に強い相互作用があり、マイクロ秒の時間スケールでは、イオンはリン脂質分子の相分離に応答して再分布することを明らかにした。

相分離後のリン脂質二重膜直上の Na^+ の濃度分布を図 1 (c) に示す。グラフ横軸は負に帯電した DAPG の局所的な濃度とした。図中の赤点で示したシミュレーション結果から、負に帯電した DPAG の濃度（膜上の表面電荷）が大きくなると、膜上のカチオン濃度も大きくなる傾向が見られた。Poisson–Boltzmann 方程式（図中 PB で表示）と比較すると、シミュレーション結果とは一致しなかった。そこで、イオンを点電荷ではなく、直径 0.9 nm の排除体積を考慮した修正した方程式を用いると (図中 a=0.9 nm で表示)、シミュレーション結果と良い一致を示した。この結果から、水溶液におけるイオン間相互作用の重要性が示唆された。今回の結果をまとめ、2022 年度に論文投稿し、2023 年度に出版された。

1. *Yuji Higuchi, Klemen Bohinc, Jurij Reščič, Naofumi Shimokawa, and Hiroaki Ito
“Coarse-grained molecular dynamics simulation of cation distribution profiles on negatively charged lipid membranes during phase separation”
Soft Matter 19, 3640–3651 (2023).



【図 1 】(a) リン脂質分子の構造式。(b) DPPC:DAPG = 1:1 混合における相分離プロセス。
(c) 負に帯電したリン脂質分子の局所的な濃度 φ_i に対するカチオン濃度。

7.12　小出　洋 〈情報システムセキュリティ研究部門 教授〉

研究目的及び成果等

システムは運用開始後の構成変更や設定変更などの要因により、管理情報と実体が乖離する事態が発生することがある。これにより実体に合わせた適切なセキュリティ管理ができなくなり、インシデントの発生確率が高くなるとともに、発生時の対応が困難になることがある。このような事態を防ぐために、システムやネットワークの構成や設定といった状態情報を定期的に把握し、実体に則したセキュリティレベルを評価して対策を行う必要がある。この状態情報の把握とセキュリティレベルの評価を自動かつ定期的に行う手法について検討する。

基本的な研究の進め方は、まずこの目的に資することができる複数の要素技術に関する研究を進めている。これらの要素技術が利用できるという前提で「システムの状態把握とセキュリティレベルの評価を自動的に行う」ことができるシステムを提案・実装・評価までを行う。これはこれらの要素技術が実際的な情報システム上に適用する場合でも有効であること評価できることになる。これらの要素技術に関連する研究を含め、研究テーマは以下の通りである。

1. Moving Target Defense（MTD; 移動標的防御）に関する研究：企業内の情報システムのように境界が明確であり、情報システム内で使用するパラメータを制御可能な場合に移動標的型防御の適用は、サイバー口撃の攻撃者側の調査に要するコストを大幅に増やすために有効である。また攻撃の検出にも有用であるため、本研究の目的にも即している。

   本年度は最終的には本研究における提案システムに利用できることを視野にいれた、プロキシを用いたネットワークレベルの MTD[2,7]、および、システムコールレベルの MTD[8] についての研究を進めた。

2. 脅威トレースに関する研究：小出らが提案している脅威トレースは、大規模で複雑な情報システムにマルウェアやサイバー攻撃に使われる脅威が侵入したときにどのような挙動をとるのか自動的に解析することにより、サイバー攻撃の防御や情報システムの運用や設計に役立てることである。脅威トレースの研究で得たさまざまな知見は本研究の目的に資することができる。

   本年度は脅威トレースの高度化と新しいアクタモデルへの対応などの複数の課題に取り組んだ。

3. 安全な Web アプリケーションのためのフレームワークに関する研究：情報システムの重要な要素に Web アプリケーションが挙げられ、そこに攻撃対象となる機密情報や個人情報などが集められるため、しばしばサイバー攻撃の対象となる。Web アプリケーションは OR マッピング、データベース、認証機能などの一般的に良く使われる機能が実装された Web アプリケーションフレームワークと呼ばれるライブラリやツールを使って構築される。サイバー攻撃から Web アプリケーションを防御したり、サイバー攻撃を検出したりする機能は、Web アプリケーションフレームワークに備わっているべきものである。そこで本研究の目的達成のための要素技術のひとつとして、Web アプリケーションフレームワークの機能として追加すべきサイバー攻撃防御・検出機能を検討している。

   本年度は、Web アプリケーションにサイバー攻撃が行われた場合に攻撃を適切にハニーポットに誘導する新しい仕組み [9] と、Web アプリケーションに脆弱性が作り込まれた場合にそれを静的な解析と動的な解析を組み合わせて自動的に検出する仕組みに関する研究を行い、さら

にクラウド上で複雑な情報システムを構成する Web アプリケーションの場合に攻撃に対応してシステムの構成変更まで考慮する手法を提案した [10]。

4. 情報の信頼性を担保する新しい情報送受信システムに関する研究：世の中で出回っている、特に SNS などに散在する情報の中にはしばしば信頼できないデマ情報やフェークニュースも存在しており、それらの情報により混乱を招いたり、信頼性を損ねたりすることがある。

   本要素技術に関する研究の目的は、そのような情報を適切に評価できるようにすることである。そこで、情報を発信する複数の「発信者」および情報を受信する複数の「受信者」の両者が互いに評価できる PKI（Public Key Infrastructure）と同様の仕組みを採用した仕組みを提案し、モデルを構築し、そのモデルを用いたシミュレーションを行い、評価までを行った [3,4,6]。

   本要素技術は、一見すると本研究の目的とは無関係のように思える。しかし、組織活動の主体はその構成員たる人間であり、組織活動における情報発信の基本的な発信源は人間であることから、組織の中で利活用される情報の信頼性を担保する仕組みを検討することは不可欠である。

以上の研究の他、情報システムにおけるサイバー攻撃の検知に利用可能な機械学習に関連する研究 [1,5] も実施しており、本研究で提案するシステムに適用することを検討している。

査読付き国際会議、査読付きジャーナル

[1] Mariama Mbow, Kouichi Sakurai, Hiroshi Koide: Advances in Adversarial Attacks and Defenses in Intrusion Detection System: A Survey, Communications in Computer and Information Science 196-212 2023 年 1 月.

[2] Kouki Inoue, Hiroshi Koide: Detection and Isolation Malware by Dynamic Routing Moving Target Defense with Proxies, Proc. 9th Annual Conf. on Computational Science & Computational Intelligence (CSCI'22) 2022 年 12 月 .

[3] Shugo Yoshimura, Kouki Inoue, Dirceu Cavendish, Hiroshi Koide：A New Secure Publication Subscription Framework with Multiple Arbitrators, International Journal on Advances in Security 15(3&4) 96-105 2022 年 12 月.

[4] Shugo Yoshimura, Kouki Inoue, Dirceu Cavendish, Hiroshi Koide：Secure Publication Subscription Framework for Reliable Information Dissemination, Proc. The 2022 IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications IARIA Congress 2022 2022 年 7 月 .

[5] Mariama Mbow, Hiroshi Koide, Kouichi Sakurai: Handling class Imbalance problem in Intrusion Detection System based on deep learning. Int. J. Netw. Comput. 12(2) 467-492 2022 年 .

7.13　櫻井　大督 〈汎オミクス計測・計算科学センター 准教授〉

今年度は、音楽と AI を組み合わせる研究を発表した。それが「GéneLive! Generating Rhythm Actions for Love Live!」であり、これは 2023 年 2 月に Association for the Advancement of Artificial Intelligence が開催した、第 37 回 AAAI Conference on Artificial Intelligence で発表された。この研究は、リズムアクションゲーム向けの「譜面」を生成する AI の開発を目指したものであり、近年注目を集める生成 AI を応用した。音楽 AI の研究自体がまだ探求の余地が多い分野であることを考えると、その進展は特に意義深いものと言えよう。また、当センターのスーパーコンピュータを駆使したことで、時間を割いてチューニングを行うことが出来、性能が向上した。すなわち、スパコンが現実社会の課題を解決した好例と言える。その成果は、世界中の人が利用できるように公開した。それと同時に、共同研究先の企業にとっても、特にノウハウ面で貢献できたのではないかと考える。

リズムアクションゲームにおける譜面とは、プレイヤーがゲーム内でタップすべきタイミングや位置の指定のことである。リズムアクションゲームのプレイヤーはこの指定に従って、音楽とマッチするようにリズムを刻んでいく。今回は、世界展開をしている実際のゲームタイトルのための研究となった。

AI で譜面を生成をするとは具体的には、音楽のリズムやメロディなどの要素を解析し、タップするタイミングや位置を自動的に創出することである。近年、AI は文章生成や画像生成など様々な分野で活用されているが、音楽分野での応用はまだ発展途上であり、さらなる研究が求められている。

特に注目すべきは、この研究が民間企業で実際に運用され、大幅なコスト削減に寄与した点である。譜面の生成に関連するコストと労力を大幅に軽減することができ、AI の力を利用して新たな価値を創出することができた。その中心となる手法は、曲の拍位置という比較的容易に取得できる情報を利用したことである。これにより、安価な追加コストで、飛躍的な性能向上を実現することができた。

さらに、時間についてのマルチスケール解析を導入したことで、長い時間を観察した際に得られる特徴を学習することが可能になった。例えば、秒規模の時間進行を分析し、その結果をもとに譜面を生成している。これにより、単なる瞬間的なパターン認識から一歩進んで、曲の流れを把握し、それに基づいて譜面を生成することを狙った。これは、リズムゲームにおいてプレイヤーが楽曲の全体的な流れを感じるという重要な要素を、AI が補助することを可能にするアプローチである。

GenéLive! Generating Rhythm Actions in Love Live! Takada, A., Yamazaki, D., Yoshida, Y., Ganbat, N., Shimotomai, T., Hamada, N., Liu, L., Yamamoto, T., Sakurai, D. Presented at AAAI 23. In print. Preprint: https://arxiv.org/abs/2202.12823