

2.4 コンピューティングアーキテクチャ

ここでは、コンピューターの使い方から見た、大きな構造について技術動向を俯瞰する。CPUのインストラクションセットや、コンピューターそのもののハードウェア構造などには立ち入らない。性能向上、計算負荷に応じた構成、用途に応じた構成、新しい応用の開拓などの技術課題について動向を把握し、今後の展開について検討する。

(1) 俯瞰構造

ここでは、コンピューティングアーキテクチャの視点からその技術をデバイス層、分散処理基盤層、サービスプラットフォーム層、応用、サービス層の4層に整理した。俯瞰構造図を図2-4-1に示す。今後のコンピューティングについて考えると、サイバーの世界だけでなく、フィジカルの世界との連携も重要になる。そこで、フィジカル世界との接点であるデバイス層を一番下に据えている。ここには通信基盤やセンシング、アクチュエーションなどの機能が並び、サイバーとフィジカルの融合を実現する。その上に、フィジカルな制約があることを前提としてコンピューティングのあり方を考える分散処理基盤がある。ここまでの情報通信・処理の基本的な機能を提供する。

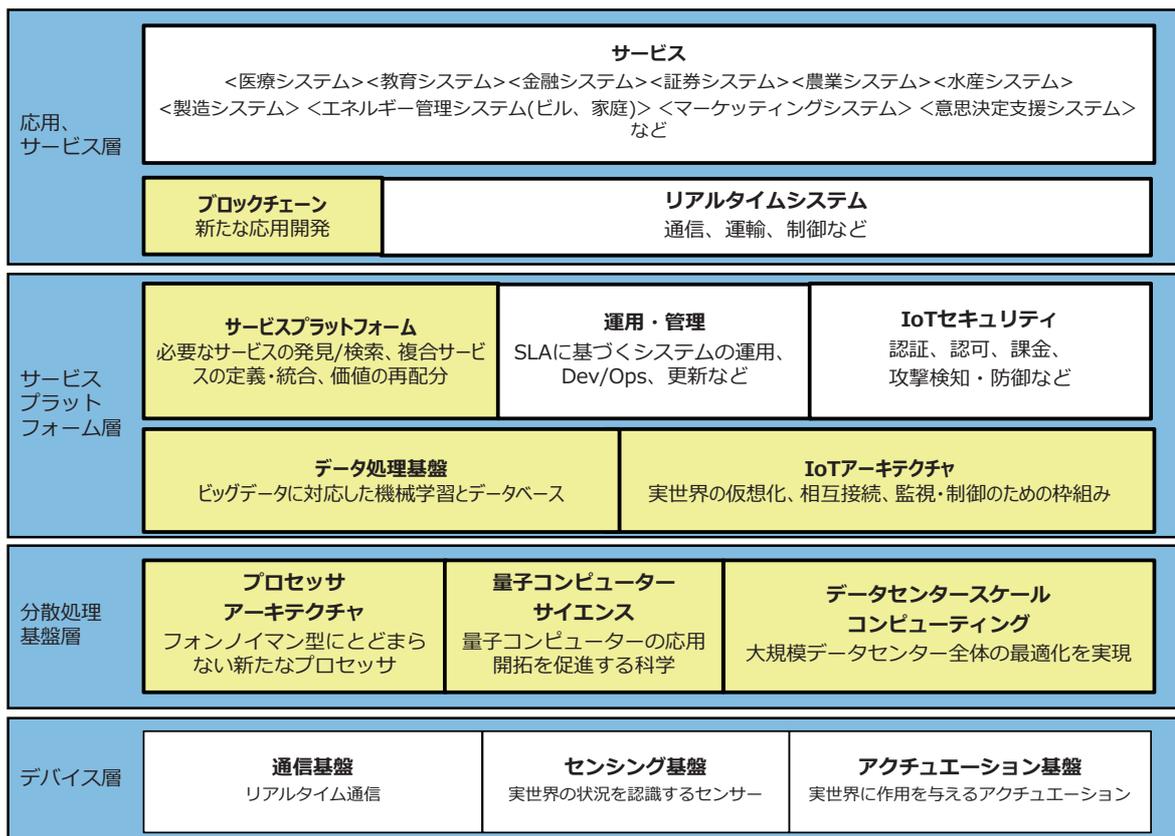


図2-4-1 コンピューティングアーキテクチャ区分俯瞰図(構造)

さらにその上に、多様な応用を載せるためのベースとしてのサービスプラットフォームが位置する。ここでは、ある程度応用を意識したシステムの構成や運用管理の手法などが議論の対象となる。

さらに最上位には応用やサービスそのものが位置する。公共的なサービス・システムや、企業が運用するサービス・システム、それらの融合したものや、どちらでも使われるものもある。また、特にリアルタイム性を重視する交通や運輸、通信などはIoT (Internet of Things) における重要な応用領域である。

(2) 時系列

これらの技術要素をコンピューターが誕生して以来の時系列の流れとしてとらえる (図2-4-2)。最初は1台のコンピューターを使うところから出発したが、すぐに複数のコンピューターを連結して使うようになった。当初は企業内でのコンピューターネットワークであったが、大規模データセンターが各地に建設されるようになり、CPU、記憶装置、通信装置などを適切に配備し運用するための技術開発が行われてきた。

さらにインターネットが普及するにつれ、ネットワーク接続されたコンピューティング環境が広く一般に使われるようになってきた。特に、クラウドコンピューティングが一般的になり、スマートフォンなどのデバイスとクラウドコンピューティングの組み合わせにより様々なサービスが提供されるようになり、そのためのソフトウェア基盤整備も進んだ。

また、IoT/CPS (Cyber Physical Systems) と言われる、フィジカル世界とサイバー世界の融合領域においては、その計算内容や負荷、反応時間などに応じて、どこにデータを置きどこでどのタイミングでどの処理をするかといった柔軟な構成が求められ、それを可能にするIoT/CPSアーキテクチャが重要になる。特に、フィジカルデバイス付近で処理を行うエッジコンピューティングは今後の発展が望まれる。

上位のサービスや応用と、コンピューティングを接続するのがサービスプラットフォームである。ハードウェアやソフトウェアの隠蔽化により、下位層の構成を意識せずに様々な応用やサービスを実現することができる。上位層から見て、このプラットフォームの出来栄が、提供できるサービスの品質を大きく左右することになる。北米を中心とする大手ITサービス企業は、多面的市場を対象としたプラットフォームを掌握し、スケーラブルなビジネスを実現している。このような動きがIoT/CPSを通じて、フィジカル世界にも広がることは容易に想像される。今後のあらゆるビジネスにおいて最も重要なレイヤーになる可能性がある。

UBERやAirBnBに代表される、シェアリングサービスが広まっている。既存のサービスに満足できないユーザからの支持を受け、今後も様々な局面でシェアリングやマッチングのサービスが広まると期待される。また、ブロックチェーンを利用した仮想通貨やスマートコントラクトなど、連携の広がり観点で新たな展開も見せつつある。新しい応用を考えることが、下位層のサービスプラットフォームや分散処理基盤に対して大きな影響を与える。必ずしも新たな応用のすべてが予想できるわけではないが、その可能性を検討しておくことは、今後のコンピューティングアーキテクチャの方向性を考えるうえで役に立つであろう。

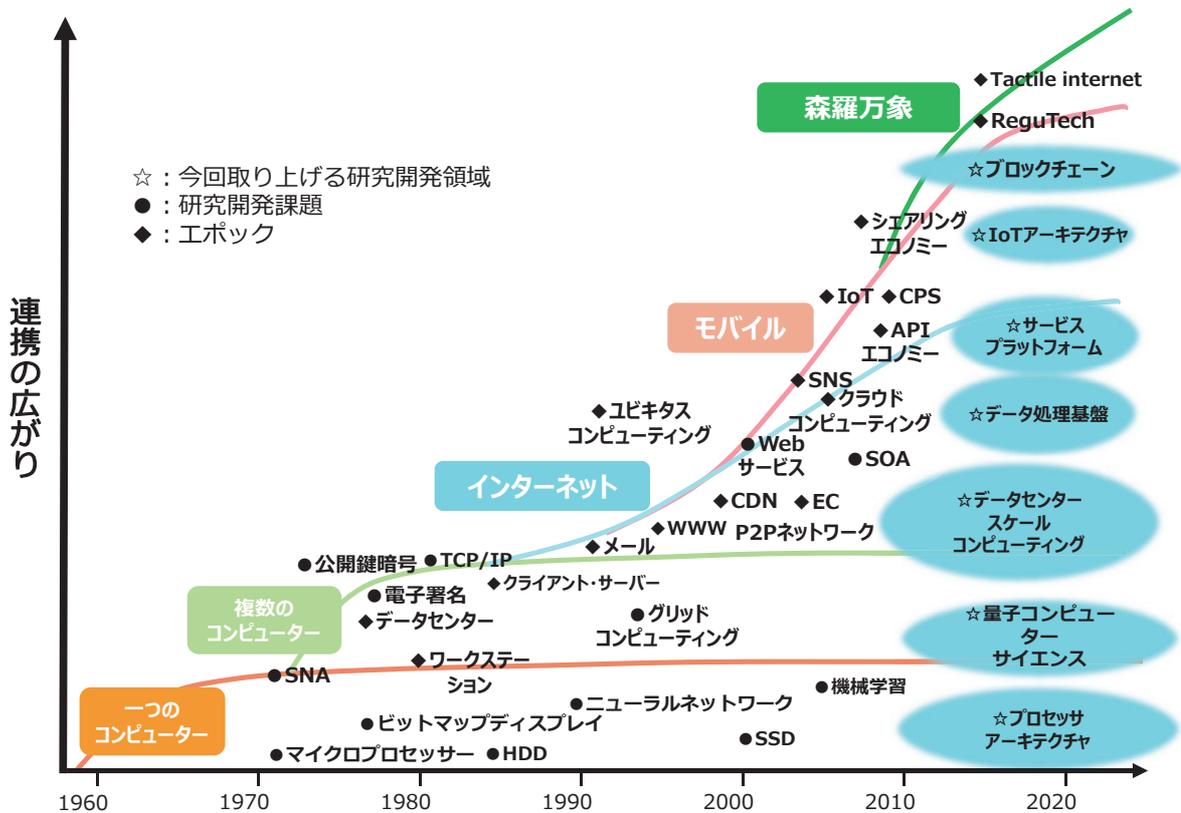


図2-4-2 コンピューティングアーキテクチャ区分俯瞰図(時系列)

本節の構成は以下のようになっている。2.4.1では新しいプロセッサの動きについて述べる。これまでムーアの法則に支えられて進歩してきた汎用プロセッサは微細加工だけに頼る性能向上は限界に達しつつある。そこで、新たなプロセッサとして、布線論理型やニューロモーフィックなどの新しいアーキテクチャのプロセッサが登場している。

さらに、従来とは全く異なる原理で動作する量子コンピューターの登場が期待されている。2.4.2では、基礎研究段階にある量子コンピューターを、コンピューターたらしめる計算機科学の観点から技術動向と課題について述べる。

米国大手IT企業はそれぞれに大規模なデータセンターを運用し、ビジネスに活用している。そこにはコンピューター単体の作り方とは全く異なる技術が存在する。2.4.3においてはそれらの技術について述べる。

大規模データ処理技術の進展が現在の人工知能技術の発展や、IoTへの期待を高めている。大規模データ処理のためには大きく分けて、計算処理そのものとデータベースがある。これらの技術について2.4.4で俯瞰する。

一方で、クラウドコンピューティングやIoTは計算処理そのものもさることながら、さまざまなサービスを結びつけ、新たなサービスを創りだし、それらを人々に届けることが重要である。そのためには、サービスプラットフォームが重要な役割を果たしている。2.4.5ではサービスプラットフォームの動向に注目する。

モバイルネットワークの進歩、普及につれて、現実世界のものやサービスと、サイバー世界が融合し始めている。この動きは農業から工業、サービス業まですべてのセクターで起きて

俯瞰区分と研究開発領域
コンピューティングアーキテクチャ

いる重要なトレンドである。そこには、IoTをどのように設計すべきかというアーキテクチャと、物理世界とサイバー世界を結びつけるデバイスが重要な役割を果たす。それらについて、2.4.6において述べる。

ビットコインをはじめとする仮想通貨が注目を集めている。その基本技術であるブロックチェーン技術はそのほかにも多くの可能性を持っている。2.4.7では分散システムやP2Pネットワークとしてのブロックチェーン技術に着目し、その技術の方向性や応用について考えてみる。

2. 4. 1 プロセッサアーキテクチャ

(1) 研究開発領域の定義

コンピューティングにおいてプロセッサは中心的な役割を果たし、長らくフォンノイマン型アーキテクチャが大勢を占めていた。アーキテクチャ (Architecture) という言葉は、元来は建築学の分野において建築様式を意味する言葉であるが、情報処理分野では、計算機ハードウェアの基本様式、基本構造、設計思想などを指す言葉として使われている。ソフトウェアは「アーキテクチャをターゲットとしてコンパイルされる」ものであり、ハードウェアは「アーキテクチャをもとにしてデザインされる」ものであると理解することができ、ソフトウェアとハードウェアとを結びつける抽象モデルがアーキテクチャであるといえる。その位置付けは極めて重要であり、プロセッサを特徴付ける概念である。

(2) キーワード

フォンノイマン型アーキテクチャ、ドメインスペシフィックアーキテクチャ、深層ニューラルネットワークアクセラレータ、リコンフィギュラブルコンピューティング、インメモリーコンピューティング、エッジコンピューティング

(3) 研究開発領域の概要

[本領域の意義]

プロセッサにおけるアーキテクチャ研究は、1980年代から90年代にかけて、CISC(Complex Instruction Set Computer) 対 RISC(Reduced Instruction Set Computer) アーキテクチャ論争、RISC アーキテクチャをベースにしたプロセッサの高実行効率化技法、命令レベル並列化、スレッドレベル並列化等の並列実行手法などの研究で大いに盛り上がった。その後、ムーアの法則 (トランジスタサイズは 1.5 年で 1/2 になる) に従ったプロセッサ単体性能の着実な向上の勢いに隠れ、アーキテクチャ研究は次第にその輝きを失っていった。しかし、2010 年頃より、主に 1) ムーアの法則に陰りが出たこと、2) アーキテクチャの工夫を必要とする新しいタイプの情報処理課題がメインストリームになったこと (後述)、の二つの事象が並行して進行し、特にここ数年は「アーキテクチャ研究の黄金時代」とも呼ばれる活況を呈している。Society 5.0 というキーワードで近未来の超スマート社会のビジョンが産官学で議論されているが、その議論は、情報処理能力のこれまで通りの指数関数的な発展を前提にしている。その前提を支えてきたムーアの法則の今後が心もとない現状においては、アーキテクチャ技術の果たすべき役割は大きい。

[研究開発の動向]

コンピューティングアーキテクチャは、いわゆるフォンノイマン型を王道として発展してきた。これは、メモリー内に蓄えられた命令列 (処理プログラム) を順次解釈・実行していくことを基本的特徴とする手続き処理型のアーキテクチャであり、チューリングマシンを源流とする極めて強力な問題記述能力・汎用性を誇る。1980年代に、多様なプログラムをより少ない命令数で実行することを目的として命令数が膨れ上がってしまった IBM 等の汎用コンピューター (CISC) に対するアンチテーゼとして、アーキテクチャを単純化・規則化して命令数

を減らしたマイクロコンピューター (RISC) が提案された。RISC は実行命令数は増えるものの、命令当たり実行時間の短縮によりプログラム処理性能が向上することが定量的に示され、脚光を浴びた。ムーアの法則の力を大いに借りて、クロック周波数向上により性能向上を図る RISC ドリブンのアプローチが、その後のアーキテクチャを席捲することとなった。

フォンノイマンアーキテクチャでは、処理プログラムと処理データの双方をメインメモリーに蓄えるため、頻繁なメインメモリーアクセスが性能律速要因になる (フォンノイマンボトルネック) ことが知られている。RISC アーキテクチャ登場以来のアーキテクチャ研究の主要な分野の一つは、このボトルネックを緩和するためのメモリーシステム階層に関するものであり、キャッシュメモリーの工夫やその他様々な命令・データのバッファリング手法が提案されてきている。その他の主要分野としては、手続き型処理の根幹となる分岐命令の先読み・予測、制御ハザードの回避、複数命令並列実行や複数スレッド (スレッドとは一塊の手続きのこと) 並列実行、プロセッサを多数並べた大規模並列システム、等が挙げられる¹⁾。

フォンノイマン型に代わる「非ノイマン型」のアーキテクチャ思想を打ち立てる研究も古くから続いている。その一つは、1980年代から90年代にかけて盛んに研究されたデータフローアーキテクチャである。その基本思想は入力データが揃って実行可能になった命令から実行する点にあり、あらかじめ定められた手続き順に命令を実行するフォンノイマン型に比べると、自然に並列化が可能というメリットがあった。ムーア則に基づく単体プロセッサ高速化の波と、当時の処理対象ワークロードが手続き処理型向きだったことで、情報処理アーキテクチャの主流とはならなかったが、様々な並列化技術としてプロセッサ内に埋め込まれる形で、現在でも広く影響を与えている。その当時、電総研 (現産総研) を始めとして日本でも有力な研究がいくつも進められ (SIGMA-1²⁾, EM4³⁾ 等)、日本のデータフロー分野の技術・アイデア・知見の蓄積は厚い。

FPGA (Field Programmable Gate Array) は、ユーザーが手元で自在に回路を実装できる集積回路として、ハードウェア設計のプロトタイプ目的で1985年に登場し発展してきた。視点を変えて、所望の情報処理をソフトウェアプログラムにではなくハードウェア構造に設計することを考えるならば、FPGA は新たなコンピューティングデバイスと考えることもできると登場当初から提唱されていた。トランジスタ微細化の進展につれ FPGA に搭載できる回路規模が爆発的に増大し、特に2010年頃からはこの「FPGA コンピューティング」の考え方が実用的な意味を持ち始めている。

FPGA コンピューティングは、あくまでプロトタイプ目的だった FPGA の別用途利用であり、コンピューティングに使うならばそもそもプログラマブルハードウェアのアーキテクチャから再定義すべきと考える研究が1990年代から2000年代にかけて盛んに進められた。一つの方向性は、1-2 バイトのデータ処理に適した粗粒度の演算器アレイ (Coarse Grained Reconfigurable Array; CGRA) アーキテクチャであり、もう一つは動的再構成アーキテクチャである。後者は、ソフトウェアにおける仮想メモリーの考え方にちなみ、ハードウェアを仮想化することで汎用性を高めようとするアプローチであり、特に日本で研究が盛んに進められた (慶応大学 WASMII⁴⁾, NEC (現ルネサスエレクトロニクス) の動的再構成プロセッサ DRP⁵⁾ など)。これらの分野はリコンフィギュラブルコンピューティングと呼ばれている (FPGA コンピューティングもその中に含んで使われる場合が多い)。

コンピューターの出力を人間が視覚的に理解するために必要となるのがグラフィクス処理

であり、GPU(Graphics Processing Unit)はその専用アーキテクチャとして発展してきた。グラフィクス処理には、画素、線分、頂点、視線方向など様々なレベルでデータ並列性が存在するため、主にSIMD(Single Instruction Multiple Data)型のデータ並列アーキテクチャとして進展してきている。既にコンピューターに組み込まれたGPUをグラフィクス目的以外でも使用して他のデータ並列性の高い応用を処理できるように、2010年頃からいわゆるGPGPU(General Purpose GPU)アーキテクチャやその利用環境が広まってきた(GPUコンピューティング)。

信号処理分野でも独自のアーキテクチャが発展してきた。信号処理には積和演算が演算の大半を占めることや、あらかじめ静的に処理時間を計算できるリアルタイム性が要求されるという特徴があり、これに応え汎用プロセッサから分化して誕生したのが信号処理プロセッサ(DSP)アーキテクチャである。主にベースバンド信号、音声、画像などが処理対象であり、特に静止/動画像を加工したり圧縮・伸長したりする処理では、2次元画像を効率よく処理するための様々なアルゴリズム・アーキテクチャ連動の工夫が創案されてきており、イメージ処理プロセッサ、ビデオ処理プロセッサなどと呼ばれている。

これらコンピューターから出発したアーキテクチャ以外に、回路の集積度がある程度進んできた段階で、それをアーキテクチャに対する境界条件の大きな変化ととらえ、集積回路の効率実装の観点からアーキテクチャを作り直そうと考える研究分野が80年代に勃興した(VLSIアーキテクチャ)。特に、フォンノイマンボトルネックの解消を狙ってメモリーとロジックが一体となったインメモリー型の処理を標榜するケースが多く、知能メモリーアーキテクチャと呼ばれている⁶⁾。メモリーアレイ内で演算を行うことから、データの移動が少なく並列性を高めやすいという特徴があるが、応用が限られるという難点があり、大きなブレークスルーを起こすには至っていない(部分的にシステムLSIに取り込まれることはある)。

また、同じく集積回路ドリブンで、正統的なアーキテクチャ研究からはみ出た研究としてニューロモルフィックアーキテクチャが挙げられる。1980年代の第2次ニューラルネットワークブームの際に、網膜神経回路のアナログ集積回路化で注目を集め、シナプスの動作を精密に模倣する回路の試作などが報告されているが、実用化とは距離のある研究であったため、単発的な研究にとどまっていた。しかし、近年になり人工知能分野において注目を浴びるようになり、IBMのTrueNorth、マンチェスター大学のSpiNNaker(Spiking Neural Network Architecture)、IntelのLoihiなど機械学習のアクセラレーターとして開発が進められている。

従来のコンピューターとは異なる計算原理で動作し、問題によっては圧倒的な高速化を実現すると期待されているのが量子コンピューターである。1980年代に理論的可能性が示され、その後、因数分解への適用可能性、量子誤り訂正符号の提案があり、2000年代には量子コンピューターの研究が活発化した。スケラビリティを確保する技術的な見通しの悪さから研究開発は停滞していた。近年になり、ハードウェア技術や量子誤り訂正符号などの進展により、その可能性が再認識されている(詳細は、2.4.2を参照)。

(4) 注目動向

[新展開・技術トピックス]

現在のアーキテクチャ研究の活況は、情報処理性能向上に対する社会的要求に応えるためには今後アーキテクチャで差分を産み出すしかない状況を反映したものである。一方、時代の変

化により情報処理の対象ワークロードが変化することで、アーキテクチャの工夫で性能向上ができる余地が生まれたからでもある。

その一つは、ビッグデータを活用しクラウドサービスを支える大規模分散並列コンピューティング技術であり、それを先鋭化したデータセンタースケール・コンピューティングアーキテクチャの考え方である⁷⁾。すなわち、今やネットワークでつながった巨大な数のコンピューティングノードの集合体そのものがコンピューターシステムであり、その構成のみならず、空調を含めた電力モデル、故障に対する冗長性、機器のライフタイムマネジメント等、システム全体のオペレーション最適化を考えるとアーキテクチャの一つの大きな分野となっている。

もう一つの分野がドメインスペシフィックアーキテクチャの新展開である⁸⁾。その背景には、機械学習、深層ニューラルネット (Deep Neural Network: DNN)、大規模グラフ処理等に代表されるビッグデータ時代の新たな情報処理ワークロードが、従来の手続き型処理から離れ、構造型処理に適した特徴を有するようになってきている点が大い。例えば、DNNは、大量・多層に並べられたニューロン間の複雑な結合網という「構造」の中に入力データストリームを流し込んで学習や推論を行うことを特徴とする。処理の中に、分岐を含む手続きはほとんど存在せずDNNという構造そのものを並列ハードウェア構造の上に適切にマッピングすることで大幅な処理能力向上を見込むことができる。このような処理対象領域の特徴をアーキテクチャに反映させることで、大幅に処理効率を向上させることがドメインスペシフィックアーキテクチャの狙いであり、前述のグラフィックス処理、信号処理、イメージ/ビデオ処理などはその走りともいえる。なお、プログラミング言語の世界でも、アーキテクチャの世界の動きに呼応して、ドメインスペシフィック言語 (Domain Specific Language: DSL) が発展していることも注目される。

深層ニューラルネット (DNN) アクセラレーター

深層ニューラルネット (DNN) が画像分類精度で従来手法を大きく超えることが2011年に報告され、本技術は一躍脚光を浴びることとなった。その成功の鍵となった学習手法は1980年代に提唱されたバックプロパゲーション (BP) 技術であるが、大規模学習データ、高性能計算機、様々なBP改善手法 (いわゆるディープラーニング/深層学習技術) 等が相俟って急速に技術発展し、今や多様な応用分野 (画像・音声認識、自動翻訳、自動運転、等) でDNN活用が広がっている。また、DNNの学習・推論処理の加速・低エネルギー化を目指して多くのDNN処理エンジンが提案され (Google社TPU⁹⁾、MIT Eyeriss¹⁰⁾、等)、新しい情報処理アーキテクチャ技術として大きな注目を集めており、ドメインスペシフィックアーキテクチャの代表的な存在であるといえる。膨大な並列性を有するという点でGPUコンピューティングがまずその中心的アーキテクチャとなり (特に学習側)、エッジ側での推論処理を対象として、組み込み機器 (特に画像処理) の積和演算アクセラレーターとして発展してきたDSPベースのアプローチも提案されている。また、構造型の情報処理であるという特徴に注目して、データフローマシンをベースとしたものや¹¹⁾、FPGAコンピューティング¹²⁾、リコンフィギュラブルコンピューティング¹³⁾ など、様々なアプローチがしのぎを削っている状況である。国内では、東京工業大学がFPGAコンピューティング¹⁴⁾、北海道大学がリコンフィギュラブルコンピューティング¹⁵⁾ベースの研究を活発に進めている。また、産業界ではルネサスエレクトロニクス社が動的再構成プロセッサをDNN処理の差別化エンジンとする技術を発表し¹⁶⁾、注目を浴びている。

ニューロモルフィックハードウェア

DNN の興隆の影響を受けて、集積回路の上で生体神経回路網の動作を出来る限り精密に模倣しようとするニューロモルフィックハードウェア分野も活性化している (DNN アクセラレーターと混同される場合が多いが、区別して理解する必要がある)。生体模倣の目的については慎重に考える必要がある (例えば鳥を忠実に模倣しても飛行機は実現できない) が、脳が DNN より桁違いに (一説に 10^4 倍) エネルギー効率が良い理由を探求し、その本質を新しい時代のアーキテクチャとして昇華していく方向の研究ならば工学的な意義も持ちうる。この分野では、IBM 社の TrueNorth¹⁷⁾ や、清華大学の Tianji¹⁸⁾、Intel 社の Loihi¹⁹⁾ などが知られている。これらはデジタル回路を採用しているが、不揮発性メモリーを用いたアナログ回路アプローチも、特に新規デバイスの出口戦略的な位置づけで、活発に研究されている。

アニーリングマシン (量子、非量子)

DNN の勃興と並行して、種々の組合せ最適化問題を二値スピン格子のイジングモデルにおけるエネルギー最小化問題に置き換え、その近似解を求めるアニーリング計算機分野も広く注目を集めている。格子状に並べられ互いに相互作用するスピンの安定状態 (すなわちエネルギー最低状態) に自然に収束するという物理現象を情報処理と見なし、短時間で質の高い近似解を得ようとする方法と理解できる。基本的には物理現象を利用して情報処理を実現するナチュラルコンピューティングの流れを汲むものであり、これまでに量子現象を使うアプローチ²⁰⁾ と、集積回路で疑似的に再現するアプローチ^{21),22)} とが提案されている。「量子アニーリング」の原理は 1998 年に東工大・西森教授が発表したことで知られ、量子力学的なトンネル効果によりエネルギー極小値にはまらずに最低状態 (= 与えられた最適化の解) を探索できるという特徴がある (ただし、実際の D-wave マシンはこの「量子アニーリング」の原理とは異なる動作をしていると考えられている)。一方、量子効果に頼らなくとも、成熟した集積回路技術とアーキテクチャの知見を活かし、スケーラビリティ、結合数、結合の階調などの観点で量子アプローチよりも実用的な計算機として開発を進めているのが日立や富士通などである。

量子コンピューター

従来のコンピューターの論理素子 (bit) では「0 か 1 か」の 2 状態の情報を計算に用いるのに対し、量子コンピューターでは「0 でありかつ 1 でもある」状態を任意の割合で組み合わせた量子ビットを用いる。量子コンピューターの計算原理としては、量子ビットに位相の回転、量子もつれ、量子干渉などの量子ゲート操作をすることにより情報処理を行う量子回路型量子計算 (量子チューリングマシン) が代表的な計算原理であり実装も進んでいるが、量子断熱計算や測定型量子計算など等価な計算モデルも多く知られている。理論通りに動作すれば、現在のコンピューターよりも本質的に高速な計算が可能となると証明されているが、現在のところ、量子性に基づく量子コンピューターの高速性を実験実証するまでには至っていない。Shor の因数分解や Grover の検索などの典型的な量子アルゴリズムが要求する量子ビット数やエラー率と、現状の技術との間には大きな隔たりがある (詳細は 2.4.2 を参照)。今後、量子コンピューターアーキテクチャの研究開発の充実が期待される。

以上のような主要なドメインスペシフィックアプローチの中で、アーキテクチャ的手段と

して特に注目されているのがリコンフィギュラブルコンピューティングである。これは、HWの構造に問題を落とし込んで解くというこのアプローチの基本的特質が、構造型の情報処理ワークロードと非常に相性が良いからである。日本では、90年代から00年代にかけて様々なリコンフィギュラブルアーキテクチャが活発に研究されてきたという歴史的な経緯があり、相対的に技術・人材の蓄積が厚い分野であるということは注目に値する。

また、演算自体は単純かつ並列化しやすく、入出力データに強くバインドされたものであるという特徴から、ニアメモリーコンピューティングないしはインメモリーコンピューティングというアプローチも重要になっている。これらのアーキテクチャ概念は知能メモリーアーキテクチャとして古くから存在するが、現実的な応用の中で重要性が増してきたため改めて注目されている状況である。

さらに、クラウド一極集中に対するアンチテーゼとして、エッジコンピューティングの概念も注目されている。利点は、ネットワークバンド幅の削減、データの秘匿性や安全性の向上、リアルタイム性の向上などであるが、エッジ側の情報処理能力をどの程度持たせるべきかなど、定量的な答えが見えていないなど課題はまだ多い。日本の産学が有する強みを今後のスマート社会に生かしていくという意味では、エッジコンピューティングのシナリオが技術競争的に非常に重要なことはほぼ間違いない。これを成立させるユースケースや応用スタディ、対応する社会的プラットフォーム等の研究開発に期待が集まるところである。

【注目すべき国内外のプロジェクト】

米国では、IEEEが中心となって、Rebooting Computing キャンペーンを2013年から始めた。これに呼応する形でDARPAが各種のコンピューティングプラットフォームに関するプロジェクトを年々増やしはじめ、2018年にはこれをまとめる形で電子技術の復権を目指すERI(Electrics Resurgence Initiative)を立ち上げ²³⁾、これから数年間で1600億円もの研究費をつぎ込むと報道されている。対象は、前述のドメインスペシフィックアーキテクチャの各分野やそのLSI設計手法、テストシステム実証を中心として、それ以外にも新規半導体デバイスや3次元実装技術のシステム応用を含んでいる。

また、UC Berkeley発のイノベーションとして、ピュアなプロセッサアーキテクチャの世界で、オープンなプロセッサプラットフォームを標榜するRISC-Vアーキテクチャが急速に求心力を高めていることも注目に値する。アーキテクチャに新規性があるのではなく、寡占の度を強めるデファクト・プロプライエタリIPであるARMアーキテクチャに対するアンチテーゼとして、オープンソースIPであることが最大の特徴であり、UC Berkeley発であるという正統性を強みにMakersムーブメントの上げ潮に乗ることに成功したように見える⁸⁾。AI系ハードウェアのアクセラレーターを構成する際にもシステム全体の管理を行うプロセッサは必須部品であり、ここにARMではなくRISC-Vを選択するプロジェクトが急速に増えている。

中国では、中国政府や有力都市の行政府が、大規模な人工知能ハードウェアプロジェクトを始めている。その予算は年間1,000億円以上といわれ、米国以上の規模を誇る。清華大学にはAI/ニューロモルフィック分野のハードウェア研究センターが設立され、北京市内の狭いエリアに隣接する清華大学、北京大学、中国科学院の関係者がキャンパス周辺にスタートアップ企業を次々に立ち上げる生態系が形成されている(一説には中国では現在30を超えるAIハードウェア系スタートアップがあるとのこと)。北京は国策で直にドライブされている状況である

が、上海・深圳でも Huawei 社や BAIDO 社が中心となって、北京と同規模の民間ムーブメントが起きている模様である。

欧州は、Human Brain プロジェクト等、ニューロモルフィック系のプロジェクトが歴史的に盛んに進められてきており、相対的には現在のアーキテクチャ革新の動静からは少し距離を置いたポジションに見える。英国に位置する ARM 社は米中からの遅れに危機感を感じてこの分野の R&D に力を入れ始めている。イスラエルでは、画像処理・信号処理技術の強みを生かして、小規模ながらスタートアップ企業が蓄積し始めている。

日本では、2018 年度から文科省の戦略目標「Society5.0 を支える革新的コンピューティング技術の創出」をもとに JST において CREST、さきがけ研究領域が立ち上がり、これと並行して経産省・NEDO でも「高効率・高速処理を可能とする AI チップ・次世代コンピューティングの技術開発」事業が立ち上がった。投資規模で米中にはるかに劣ることは明白であり、日本が蓄積してきた技術的強みや産業界でのポジショニングを明確に意識した、勝てるシナリオ作りとそれにそった研究開発戦略が求められるところである。

(5) 科学技術的課題

爆発的なスマート化の進展に呼応した情報処理対象のドラスティックな変化により、情報処理アーキテクチャは今大きな変革期を迎えている。所謂人工知能 (AI) ブームの下、米国・中国を中心に活発な開発競争が数年来続いているが、今見えている AI 技術は単なる氷山の一角であり、将来にはより豊潤な知能コンピューティングの世界が広がっていると推定して研究を強力に進めなければならない。なぜならば、一つには日進月歩で過去の常識を覆し続ける深層学習技術の爆発的発展がそれを示唆しているからであり、また一つには、それが真ならば、今後数十年にわたって発展し続けるであろう新しい情報処理アーキテクチャのイニシアティブを取ることが世界的な社会のスマート化の大競争の中で決定的に重要だからである。

科学技術上の課題としては、短期的な「AI チップ開発競争」に勝つことが目標ではなく、この新しい時代に相応しい本質的で持続可能な情報処理アーキテクチャの変革を産み出すことを目標としなければならない。アーキテクチャの世界は、Winner-Take-All の世界であり、アーキテクチャ的に正しいからデファクトスタンダードになるというのではなく、近未来の応用分野に適した尖ったアーキテクチャでニーズに応え、そのニッチな応用の爆発的な拡大とともにデファクトスタンダードに成長していくという系譜を必ず辿って最終的にデファクトとなる。この観点から、エッジにおける知的なデータ処理を、そのデータ処理に適したドメインスペシフィックなアーキテクチャで、リコンフィギュラブル、インメモリー等の尖ったアーキテクチャ的な特徴を武器としながら、応用課題やソフトウェアのエコシステムと連携して発展させていくことが重要である。

(6) その他の課題

アーキテクチャ革新の好機との認識に立つ海外の著名計算機アーキテクチャ研究者は、データと研究資金を持つ Google、NVIDIA、Facebook 等の AI プラットフォーム企業を足場に次世代アーキテクチャの研究を進めている。また、米国・中国は、AI ハードウェアに 1000 億円規模の国家予算の投資を始めており、そのような企業群と国家投資余力を持たない日本の立ち遅れは大きい。コンピューター産業競争力低下の影響を受けてアーキテクチャ研究分野から

人材が流出してきた国内ではアーキテクチャ人材が払底しており、学生にも不人気な時期が長く続いていた。長らくアーキテクチャ研究を主導してきた米国では、アーキテクチャを含むコンピューター科学の分野は継続的に人気専攻であり、例えば MIT のアーキテクチャ講義では、大型教室に学生が入りきれない状況になっている。一方、半導体とコンピューター技術振興を国策に掲げる中国では最優秀の学生層がこの分野に集中している。人材や次世代教育の点でも彼我の差は非常に大きい。

このような状況で日本がとるべきアプローチは、まずキャッチアップしなければならない状況を正しく反省することを出発点に、短中期的には過去の技術蓄積を再度掘り起こしながら尖ったアイデアの創出をプロモーションする戦略が重要である。また、長期戦略的にはコンピューティングアーキテクチャ分野の若手世代の育成を目立った形で始めることだと考える。後者に関して、中国が如何に若手世代を育成し技術をキャッチアップしてきたかを正しく理解することは、重要な一手ではないだろうか。

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・アーキテクチャ分野の国際学会ではプレゼンスはないに等しく、集積回路分野では過去の影響力を辛うじて保ってはいるが、新しいムーブメントを起こすような指導的立場は持っていない。どちらの技術階層でも人材の層が薄く、特に若年層が薄い。
	応用研究・開発	△	→	・DNNのエッジコンピューティング分野ではルネサスエレクトロニクス社が Embedded AI とその差別化 IP として DRP コアを戦略的に開発・事業展開している。アニーリングマシン分野では集積回路型で日立・富士通のプレゼンスが見える以外は、総じて世界的プレイヤーとして活躍できていない。
米国	基礎研究	◎	→	・Stanford, MIT, UCB, Harvard 等の主要大学が積極的に先進技術を発信し続けている。産学連携、官学連携等も活発で研究資金や人材育成・供給の面で研究開発のエコシステムが活発に機能している。 ・DARPA の研究資金投入が突出して目立っている。
	応用研究・開発	◎	→	・Google, Facebook 等のプラットフォームがアーキテクチャ分野に投資し続け、NVIDIA も GPGPU への先行投資が実って DNN 分野でデファクト企業の位置を積極的に狙って影響力を高めている。また、多数のスタートアップ企業が誕生し、世界の技術開発をリードしている。
欧州	基礎研究	○	→	・ニューロモルフィック分野での活動が目立つ。DNN 分野では KU Lueven, EPFL 等の少数の大学が世界的に見てレベルの高い研究を進めている。
	応用研究・開発	○	→	・ARM 社がドメインスペシフィック分野に事業戦略のかじを切り始めた。 ・英国の GraphCore, イスラエルの CEVA 等、技術的な特徴が鮮明なスタートアップ企業も存在する。
中国	基礎研究	◎	→	・アーキテクチャ分野では優れた研究成果を発表し続けており、集積回路分野でもそのレベルに達しつつある。巨額の国費を投資して技術開発を振興しており、清華大学や中国科学院の成果が目立っている。
	応用研究・開発	◎	↗	・米国には劣るものの、BAIDU などのプラットフォームを有し、積極的にアーキテクチャ分野に投資している。30 社以上の AI ハードウェアスタートアップ企業が生まれているといわれており、例えば、その一つであるユニコーン企業の Cambricon 社の技術が HUAWEI 社のスマートフォンに搭載されている。
韓国	基礎研究	○	→	・アーキテクチャ分野でも集積回路分野でも、日本よりもはるかにプレゼンスが大きい存在となっている。KAIST やソウル大学がメインプレイヤー。
	応用研究・開発	△	→	・Samsung 社の研究開発動向が垣間見える程度で、産業界全体の状況は不明。

(8) 参考文献

- 1) John Hennessy and David Patterson, "Computer Architecture: A Quantitative Approach," 6th Edition, 2017, Morgan Kaufmann.
- 2) Toshitsugu Yuba, et.al., "The SIGMA-1 dataflow computer," in ACM '87 Proceedings of the 1987 Fall Joint Computer Conference on Exploring technology: today and tomorrow, PP578-585, 1987.
- 3) Yoshinori Yamaguchi, Shuichi Sakai and Yuetsu Kodama, "Synchronization Mechanisms of a Highly Parallel Dataflow Machine EM-4," IEICE Transactions, Vol. E74, No.1, pp.204-213 (1991) .
- 4) Xiao Ping Ling and Hideharu Amano, "WASMII: a data driven computer on a virtual hardware," in Proceedings IEEE Workshop on FPGAs for Custom Computing Machines, pp33-42, 1993.
- 5) 本村真人, 他, "動的再構成プロセッサ (DRP) ," 情報処理学会誌, Vol.46, No.11, pp.1259-1265, 2005.
- 6) 村岡洋一, "知的連想メモリマシン," オーム社, 1989.
- 7) Parthasarathy Ranganathan, "More Moore: Thinking Outside the (Server) Box," Google, in Proceedings of International Symposium on Computer Architecture, 2017.
- 8) David Patterson, "50 years of Computer Architecture: From the Mainframe CPU to the Domain-Specific TPU and the Open RISC-V Instruction Set," UC Berkeley, in Proceedings of International Solid State Circuits Conference, 2018. (講演ビデオ: <https://www.youtube.com/watch?v=NZS2TtWcutc>)
- 9) Norman Jouppi, et.al., "In-Datacenter Performance Analysis of a Tensor Processing Unit," Google, in Proceedings of International Symposium on Computer Architecture, 2017.
- 10) Yu-Hsin Chen, et. Al., "Eyeriss: A Spatial Architecture for Energy-Efficient Dataflow for Convolutional Neural Networks," MIT, in Proceedings of International Symposium on Computer Architecture, 2016.
- 11) Chris Nicol, "A Dataflow Processing Chip for Training Deep Neural Networks," Wave Computing, in Proceedings of Hot Chips, 2018.
- 12) Jeremy Fowers, et. al., "A Configurable Cloud-Scale DNN Processor for Real-Time AI," Microsoft Research, in Proceedings of International Symposium on Computer Architecture, 2018.
- 13) Shouyi Yin, "An ultra-high energy-efficient reconfigurable processor for deep neural networks with binary/ternary weights in 28nm CMOS," Tshinghua University, in Proceedings of Symposium on VLSI Circuits, 2018
- 14) 中原 啓貴, "FPGA を用いたエッジ向けディープラーニングの研究開発動向," 人工知能学会誌「AI 計算資源」にあたって小特集, Vol.33, No.1, pp.31-38, 2018年1月 .
- 15) Kodai Ueyoshi, et. al., "QUEST: A 7.49-TOPS Multi-Purpose Log-Quantized DNN Inference Engine Stacked on 96MB 3D SRAM using Inductive-Coupling Technology in 40nm CMOS," International Solid-State Circuits Conference, 2018.

- 16) Taro Fujii T et. al., "New Generation Dynamically Reconfigurable Processor Technology for Accelerating Embedded AI Applications," Symposia on VLSI Technology and Circuits, pp. 41-42, 2018.
- 17) Paul A. Merolla, et. al., "A million spiking-neuron integrated circuit with a scalable communication network and interface," Science, Vol. 345, Issue 6197, pp. 668-673, 2014.
- 18) Luping Shi, et. al., "Development of a Neuromorphic Computing System," in Proceedings of IEEE International Electron Devices Meeting, 2015.
- 19) Mike Davies, "Loihi: A Neuromorphic Manycore Processor with On-Chip Learning," IEEE Micro, January/February 2018.
- 20) "The D-Wave 2000Q™ Quantum Computer Technology Overview," D-Wave, 2016. (https://www.dwavesys.com/sites/default/files/D-Wave%202000Q%20Tech%20Collateral_0117F.pdf)
- 21) 山岡 雅直, "組合せ最適化問題に向けた CMOS アニーリングマシン," 日立, IEICE Fundamentals Review, Vol.11, No.3, 2018.
- 22) "AI と量子コンピューティング技術による新時代の幕開け ～デジタルアニーラが未来を切り拓く～," 富士通, FUJITSU JOURNAL, 2017.
- 23) <https://www.darpa.mil/work-with-us/electronics-resurgence-initiative>

2. 4. 2 量子コンピューターサイエンス

(1) 研究開発領域の定義

量子コンピューティング（量子計算）とは、状態の重ね合わせ、量子もつれ、量子干渉などを計算資源として、古典系では不可能な情報処理を可能とする新たなコンピューティングである。本研究開発領域は、理論的な計算モデルから、ソフトウェア、アーキテクチャ、ハードウェアなど物理学・計算機科学・電子工学の広範囲に及ぶ話題を含む。また、量子コンピューター実現に必要な様々な工学、量子コンピューター開発を通して得られる計算機科学への示唆も関連トピックスとして含む。

(2) キーワード

量子コンピューター、量子計算、量子情報科学、計算機科学、量子ビット、量子ゲート、量子回路、量子アルゴリズム、量子加速、量子プログラミング言語、量子コンパイラ、量子SDK、量子コンピューターアーキテクチャ、NISQ、量子優位性、量子誤り訂正符号、量子メモリ、量子センサー、量子通信、量子アニーリング、イジングモデル、量子シミュレーター

(3) 研究開発領域の概要

[本領域の意義]

半導体微細加工技術によるコンピューターの飛躍的な性能向上が技術的・経済的な限界に近づき、これまでのように個々のトランジスタ性能向上だけによる計算機の性能向上はもはや望めなくなってきた¹⁾。一方で、ビッグデータ処理、メディア処理、深層学習、組合せ最適化などの計算ニーズが高まり、コンピューターの性能向上に大きな社会的期待が寄せられている。このようにシーズ・ニーズの両面から、新計算原理、新アルゴリズム、新アーキテクチャ、新デバイスなど新しい計算パラダイムとその計算機システム実現技術への関心が、近年急速に高まっている²⁾。

このような背景のもと、注目を集めているのが「量子コンピューター」である。因数分解や検索などの特定の問題を効率的に計算できる量子アルゴリズムが複数知られているほか、量子化学計算や機械学習での利用も期待されている。しかし、いずれも実用サイズの計算を実行するにはハードウェア性能が不足している。量子回路モデルを中心とするハードウェアの開発目標は、量子ビット集積化と高忠実度・高操作性の量子ゲート実装、そして量子誤り訂正符号の実装による大規模化³⁾であるが、開発には2～30年程度要すると見られる。ソフトウェアやアーキテクチャの視点もまだ不足している⁴⁾。この理論・アルゴリズムとハードウェアの間の大きなギャップを埋めるには、量子情報科学と電子工学、計算機科学、数理科学などが融合した「量子コンピューターサイエンス」が必要である。本領域は、量子コンピューター実現を支える学理基盤・工学基盤として意義深い。また、量子優位性の実験検証は理論計算機科学にとって重要なマイルストーンであり、新しいアルゴリズムの発見など、量子計算・量子情報処理が従来の計算機科学にもたらすフィードバックが大いに期待される点でも意義がある。

[研究開発の動向]

これまでの研究開発の流れ

量子コンピューターの計算モデルとして現在一般的なものは、1993年に Yao により提案された量子回路モデル⁵⁾である。等価な量子計算モデルには、断熱量子計算、測定型量子計算、トポロジカル量子計算などがある⁶⁾。量子回路モデルよりも物理的に自然な（すなわち、計算機実現に妥当そうな）モデルもあるが、現在のところ量子回路モデルに基づく研究に取り組む研究者・組織が多い。

量子コンピューター研究の第1次ブームのきっかけは Shor の因数分解アルゴリズム（1994年）と Grover の検索アルゴリズム（1996年）という2大アルゴリズムの登場である⁷⁾。デコヒーレンスや量子誤りなどハードウェアの技術課題に明るい見通しはなかったものの、Calderbank、Shor、Steane らによって具体的な誤り訂正符号⁸⁾も提案され、理論的研究が2000年代初頭にかけての量子コンピューター研究の駆動力となった。米国標準技術研究所（NIST）がウェブ公開する「Quantum Algorithm Zoo」には、現在までに提案された多数の量子アルゴリズムが整理されている⁹⁾。

大規模量子コンピューターの実現には、複数の物理量子ビットから論理誤りのない論理量子ビットを構成する「量子誤り訂正符号」が鍵となる。中でも、2次元表面符号と呼ばれる符号が、エラー閾値が約1%と高く注目されている。この符号には、エラーの検出・訂正に最近傍の量子ビット間での2量子ビットゲートまでしか必要としない、2次元正方格子の各辺を伸ばすだけでエラー耐性を決める符号距離を大きくできる、などハードウェア実装面での利点もある。IBM や Google の超伝導量子ビットのレイアウトが2次元正方格子なのは2次元表面符号の実装を念頭にしているためである¹⁰⁾。

近年のトレンド

現在生じている第2次量子コンピューターブームの火付け役は、2014年のカリフォルニア大学サンタバーバラ校（UCSB）の Martinis グループによる、超伝導5量子ビットデバイスでの高忠実度（1量子ビットゲート：99.92%、2量子ビットゲート：99.4%、測定：99%）の実証¹¹⁾だと言われる。このブームは、理論・実験の両面で「量子コンピューターをいかに創るか」という工学的なフェーズに入ったことが特徴である。Google、IBM、Microsoft、Intel、Alibaba といったIT企業が量子コンピューターへの研究開発投資を拡大し、QC Ware、Rigetti Computing、IonQ、1QBit、Zapata Computing などスタートアップも次々立ち上がった。

現状では、超伝導量子ビット系では20量子ビットデバイスの動作確認までされており、50～100量子ビットのサイズでの動作検証も予定されている。イオントラップでは51量子ビットの量子シミュレーターなどが報告されている¹²⁾。このサイズは誤り訂正符号の原理実証が可能であるほか、計算能力の点での概念実証も可能だろう。ただし、ゲートのエラー率は高く、意味ある量子計算が実行できる量子回路の深さ（ステップ数）は限られる。そのため、浅い量子回路と（古典）統計処理・最適化を組み合わせる演算するアルゴリズムが精力的に探索されている。また、古典コンピューターでは量子コンピューターのふるまいを効率的にシミュレーションできないことを証明する量子優位性の検証¹³⁾も、小規模量子コンピューターで実行可能なインパクトある研究課題である。

海外・国内政策動向

量子コンピューターを含む一連の量子技術には、各国政府は競うように大規模な研究開発投資を進めている。米国¹⁴⁾、欧州¹⁵⁾、中国¹⁶⁾、英国¹⁷⁾、カナダ¹⁸⁾、ドイツ¹⁹⁾などでは今後、大規模な研究支援が見込まれる。国として早期から量子技術への注力を表明してきたのはオランダである。2013年のQuTechセンター開設に呼応するように、翌年にはオランダ政府は科学技術外交における「National Icon」に位置付け、大規模な政府投資を行うことを発表した。QuTechは量子コンピューターの重要開発拠点であるだけでなく、欧州全体の量子技術研究の象徴的な研究機関といえよう。欧州のFET Flagshipプログラム「Quantum Technology Flagship」の初回公募では、OpenSuperQとAQTIONの2つの量子コンピューター開発プロジェクトが採択された。

我が国では、2017年に文部科学省量子科学技術委員会が「量子科学技術（光・量子技術）の新たな推進方策」²⁰⁾を発表、これを受ける形で、同省は研究開発プログラム「光・量子飛躍フラッグシッププログラム（Q-LEAP）」を開始、「量子情報処理」「量子計測・センシング」「次世代レーザー」の3つの技術領域で合計20件の研究課題が採択された。また、情報処理推進機構（IPA）「未踏ターゲット事業」において「アニーリングマシン」「ゲート式量子コンピューター」の2部門でIT人材育成・支援が進められている。

（4）注目動向

〔新展開・技術トピックス〕

量子ソフトウェア開発プラットフォーム

ハードウェアの技術進展に伴い、その計算能力を最大限引き出すためのソフトウェアの重要性も増してきている²¹⁾。量子ソフトウェア開発の基盤となる量子プログラミング言語の設計は、比較的初期から取り組まれたテーマである。QCL、QPL、QMLなどの量子プログラミング言語が開発され、近年では、コンパイラをともなった量子プログラミング言語 Quipper と Scaffold の開発が注目される。また、Microsoft が C# から呼び出すことを想定したドメイン固有言語として Q# を開発・公開している。いずれの言語も、QRAM モデルでの実行を想定している。QRAM モデルは「量子データ・古典的制御」の標語のとおり、データに量子力学的重ね合わせを許すが、プログラムには重ね合わせは許されず、プログラム（命令流）は古典的なままである。入出力は古典コンピューターに対して行うため、「量子プログラム」は全て古典データで表現される²²⁾。

最近になり、実際の小規模量子コンピューター実機やそれを模したシミュレーター上で誰もが量子計算を実行できるような、具体的プラットフォームが登場した²³⁾。代表的な量子ソフトウェア開発キット（SDK）として、IBM の QISKit、Rigetti の Forest、スイス連邦工科大学（ETH）の Project Q、Microsoft の QDK、Google の Cirq、デルフト工科大学（TU Delft）の Quantum Inspire などがある。多くは、プログラミング言語とコンパイラのほか、シミュレーター、ライブラリ、検証ツール、サンプルコード、ドキュメントなどがパッケージとなっている。量子プログラミング言語としては IBM の OpenQASM のほか、Rigetti の Quil、Microsoft の Q# などそれぞれ SDK ごとで独自に提供される。IBM は量子ビット制御用の低級言語の OpenPulse も公開している²⁴⁾。関数型の量子プログラミング言語としては（Haskell をホストとする）Quipper が有名²⁵⁾であるが、上記いずれのプラットフォームでも採用され

ていない。

多くの SDK でバックエンドはシミュレーターのみである中、IBM の QISKit は、実機を利用できる点で注目されている²⁶⁾。高級言語から OpenQASM をターゲットとしたコンパイラ (Microsoft QDK ではドライバの扱い) も開発されており²⁷⁾、OpenQASM は量子回路の表現形式としてデファクト標準になりつつある。シミュレーターに特化することで高速化を図る動きもあり、京都大学藤井研究室が開発する高速量子回路シミュレーター Qulacs などが知られている。現状は多様な可能性が試されている状況であり、今後の整理・洗練に注視する必要がある。

量子コンピューターアーキテクチャの重要性

量子コンピューターにおけるアーキテクチャの概念は、ハードウェアの規模拡大とともにその重要性が認識されつつある^{28, 29)}。誤り訂正がある場合とない場合ではレイヤー構造は大きく異なり、どのように構造化するかはアーキテクチャ研究の重要なテーマである。現状の 5 ~ 50 量子ビットをアーキテクチャ概念なしにそのまま大規模化することは不可能である。とくに、構成要素の粒度・抽象度、要素間インターフェイス、古典・量子の命令フロー、量子・古典部分のインターフェイスなど、設計すべきことは多い。設計指針としては、NISQ (Noisy Intermediate-Scale Quantum) デバイスではドメイン志向で検索やサンプリングないしは量子アルゴリズムで頻出する位相推定などの特定の量子計算に最適化する方向性が考えられる³⁰⁾。大規模量子コンピューターでは誤り訂正符号の選択がアーキテクチャを決める。

これまで述べたように、量子アルゴリズムや量子プログラミング言語、量子ソフトウェア開発キット (SDK) がハードウェアの状況からある程度自由に開発されているのは、計算機と呼ぶに十分な性能のハードウェアが未だ登場していないからという見方もできる³¹⁾。高い操作性 (ゲート速度) と高い忠実度を達成し、集積化するような実装技術の開発は依然として困難を極めている。実現系としては、ゲート速度で優れる超伝導回路と、ゲート忠実度に優れるイオントラップの 2 つの系が有望視されているほか、固体系ではシリコン量子ドット系も注目されている³²⁾。量子センサーや量子通信との接続性を考えると、ダイヤモンド NV センターや光量子ビットも開発余地が十分にあると思われる。高周波回路、配線、パッケージング、低温技術など、電子工学の知見も広く活かされる³³⁾。

NISQ 時代の量子計算

エラー耐性量子コンピューターの登場にはまだ時間がかかるため、現実的に手に入るエラー耐性無しの量子コンピューター上で、エラーを許しながら、なんらかの量子優位性のある計算を実行することは重要な研究開発テーマである。近年、NISQ デバイスでの実行を考慮して、Variational Quantum Eigensolver (VQE)³⁴⁾ や、Quantum Approximate Optimization Algorithm (QAOA)³⁵⁾、Quantum Circuit Learning (QCL)³⁶⁾ などの量子・古典ハイブリッドアルゴリズムの提案が相次いでいる。これらのアルゴリズムでは、量子部分は古典最適化アルゴリズムに埋め込まれており、1 回の計算で量子部分に多くのステップが要求されない (浅い量子回路) という特徴がある。

NISQ デバイスの多くは量子ゲートのエラー率や量子ビット間の結合性が限定的であり、量子ビット・量子ゲートの性能もチップ内でばらつく。そのため、量子ビット・量子ゲートの優

先利用を決める「マッピング」に関する研究も近年進められている³⁷⁾。空間的なマッピングのほか、測定回数やノイズの大きなゲートを別のゲートの組み合わせで近似するなど、時間方向への分解と最適化も重要な課題である。

量子優位性

量子優位性 (Quantum Advantage や Quantum computational supremacy と呼ばれる) の検証は、「量子コンピューターの振る舞いが古典コンピューターでは (多項式時間では) シミュレーションできない」ことを証明しようという理論・実験研究である。アルゴリズムの実用的な意味合いはないものの、量子コンピューターの研究の重要テーマである。ランダム量子回路、ボソンサンプリング、IQP、DQC1 などのモデルがあり、Shor の素因数分解アルゴリズムなどと比べて単純な量子回路で実現可能である³⁸⁾。Google のグループはランダム量子回路の方法で実験実証しようとしている。理論的には、量子計算が古典計算より高速であることはほぼ保証されている状況であるが、具体的な問題設定での実験実証は、理論計算機科学の歴史上重要なマイルストーンである。

多くの場合、スーパーコンピューターによるシミュレーションが「実質不可能」となるような問題サイズはどの程度か、という点に関心が集まる。古典アルゴリズムの進歩やコンピューターそのものの性能向上により、この問題サイズは変化する。最近では、90 量子ビットあれば最新のスパコンでも計算が 100 年かかるとの試算もある³⁹⁾。

この観点から、そもそも NISQ ハードウェアのサイズ (たかだか 100 量子ビット) で使われる量子アルゴリズムを、通常の計算量理論で性能評価するのは適切でないといえる。例えば、古典ベストのアルゴリズムでは問題サイズ n に対し $O(n)$ の時間かかるところを $O(\log n)$ に加速する量子アルゴリズムがあったとしても、定数倍の範囲で量子加速は確認できず、古典計算の方が速いように見えることも生じうる (たとえば、 $n = 50$ については $n < 15 \log n$ で古典計算のほうが早い)。

量子コンピューターが古典コンピューターを凌駕する領域を理論・実験的に正確に把握することは、量子コンピューターサイエンスにとって極めて重要である。同時に、従来の計算量理論への新たな視点のフィードバックも期待できる。量子コンピューターの計算能力のベンチマーキングや、様々なレベルにおける検証にも有益な知見を提供してくれるだろう。加えて、量子計算を古典計算で検証できるかという問題は、計算量理論における未解決問題のひとつであり、その証明は大きなインパクトを生む。実用的な検証プロトコル実現の意味でも重要な問題である。

標準化・ベンチマーキング

IEEE Standard Association (IEEE-SA) が量子コンピューティングにかかる用語の標準化プロジェクトを推進している⁴⁰⁾。IEEE P7130 「Standard for Quantum Computing Definitions」は、トンネル効果、量子干渉、重ね合わせ、エンタングルメントなどの用語定義に加え、技術の進展に合わせた追加工業定義も想定されている。IEEE P7131 「Standard for Quantum Computing Performance Metrics & Performance Benchmarking」はメトリクスやベンチマーキングに関する標準化である。今後拡大するコミュニティ内の円滑なコミュニケーションには、定義が共有された共通言語が不可欠である。また、多様な量子コンピューター

の技術進展を定量的に評価・追跡することは今後の量子コンピューター研究開発を加速するための基盤として重要である。

量子アニーラー・量子シミュレーター

量子回路モデルに基づく量子コンピューターとは異なる計算原理で動作するコンピューターとして量子アニーラーと量子シミュレーターが挙げられる⁴¹⁾。最も大規模である D-wave Systems 社のマシンは最適化問題を横磁場イジングモデルの最低エネルギー状態探索問題として解く。量子アニーリングは組合せ最適化問題に対するメタヒューリスティックス解法であり、理想的な条件下では「量子計算」のひとつである量子断熱計算を含む広い概念と理解される⁴²⁾。この計算原理で動作するコンピューターは自然現象を利用して最適化問題の近似解を与えるアナログ量子コンピューターと捉えるべきだろう。比較的大規模の量子シミュレーター⁴³⁾や、non-stoquastic (注: sto “qu” astic は量的に見えて実は古典の確率的 (stochastic) モデルで表現可能、という意味の造語である) な効果による指数加速の達成⁴⁴⁾など、今後の発展も注目される。

[注目すべき国内外のプロジェクト]

- QuTech (オランダ): 「誤り耐性量子計算 (FTQC)」 「量子インターネットとネットワークコンピューティング」 「トポロジカル量子計算」 の3つを研究目標に掲げる欧州の量子技術研究の中心拠点。Intel や Microsoft などと共同研究を実施。
- Networked Quantum Information Technologies (NQIT) Hub (英国): 「UK National Quantum Technologies Programme (UKNQTP)」 の4カ所のハブ拠点のうち最大の拠点。Oxford 大学を拠点とし、量子コンピューターと量子シミュレーター (Quantum demonstrator) の開発が目標。
- 量子計算実験室 (中国): 中国科学院 (CAS) と Alibaba 社との MoU のもと設立された量子コンピューター開発センター。クラウド提供など活発な研究開発を進めている。量子技術としては中国科学技術大学に依拠している。
- EPiQC (米国): NSF 支援による量子情報とコンピューターサイエンスの混成チームで、実用的な量子コンピューター開発をねらうプロジェクト。シミュレーター、デバッガ、コンパイラ開発のほか、IEEE や ACM 系の国際学会でのチュートリアル実施など、アウトリーチにも積極的。
- IEEE Rebooting Computing Initiative (米国): IEEE 内のワーキンググループ。主催する国際会議 ICRC では量子コンピューター関係の発表も多い。「IEEE Quantum Computing Summit」 の開催や、「量子コンピューティングのメトリクスとベンチマークのための IEEE フレームワーク」 の公開など、活動は活発である。
- 慶應義塾大学 量子コンピューティングセンター (日本): IBM Q Network Hub のアジア地区の唯一の拠点で、実機のリモートアクセスが可能。参加企業との連携による量子ソフトウェア開発を行うほか、教育活動も熱心である。

(5) 科学技術的課題

エラー耐性量子コンピューターと現状の NISQ デバイスとの間には量子ビット数で5～6桁に渡る計算機システムとしての大きなギャップが存在している。ソフトウェアとアーキテクチャの研究開発の充実により、量子アルゴリズムから量子ハードウェアに至る量子コンピューター開発全体を強化する必要がある。とりわけ、計算機システムとして実現するような、大規模化を前提とした俯瞰的な設計・開発が求められる⁴⁵⁾。

理論・ソフトウェアではオーバーヘッドの軽い誤り訂正符号、浅い量子回路で有用な計算を行える新アルゴリズム、ハードウェアでは量子ゲートのエラー制御技術の高精度化、実装容易な集積化法の探索、量子制御部分まで含めたチップレイアウト設計など、様々なアプローチでギャップを埋めてゆく必要がある。量子回路を最適化することで誤り訂正符号のオーバーヘッドをソフトウェア的あるいはアーキテクチャ的に緩和できることもあろう。また、トポロジカル量子誤り訂正符号を採用する場合に、計算リソースの大半を占める T ファクトリー (論理 T ゲートをサポートするために必要な「魔法状態」と呼ばれるアンシラ状態の生成) などを、実行ユニットやファブリックなどとして取り出すような、アーキテクチャ志向の取り組みも必要である⁴⁶⁾。

研究開発が進捗している超伝導回路では、デコヒーレンスの理解とそれに基づく改善、制御用エレクトロニクスの開発 (低温 CMOS、超伝導回路)、量子誤り訂正符号と量子ビットレイアウト・配線のコ・デザイン、そして、量子ビットの集積化が必要である。また、マイクロ波帯で動作する超伝導回路と光量子通信 (近赤外～可視域) との間を量子情報のまま接続する量子インターフェイス技術が長期的には必要である。

(通常の意味の) ソフトウェア工学の発展も待たれる。とりわけ、量子ハードウェア制御に関するソフトウェア (ファームウェア) として、誤り訂正処理を行うプログラム、NISQ マシンでの誤り抑制方法の探索、動作検証の理論と具体的なソフトウェアツールなどは、すぐにも必要だろう。同様に、量子プログラムのコンパイラ、リソース推定・最適化ツール、最適化後の量子回路の検証ツールなども、(古典コンピューター上の) ソフトウェアとして重要である。ハードウェアとしての量子回路を検証するような理論の構築と、具体的なツールの開発も不可欠である。

(6) その他の課題

量子コンピューターの研究開発にはハードウェアからソフトウェアに至るまでの必要な全ての技術をフルスタックで用意することが重要となるが、それらに関わる機器や人材を物理的に1ヶ所に集合させることは現実的でない。したがって、多様な研究開発拠点や研究チームから成る研究開発ネットワークの構築と、その効果的・効率的な連携・協調動作のためのハブ拠点が複数必要だろう。

例えば、量子コンピューターサイエンス研究開発拠点、計算プラットフォーム運営・提供拠点、教育・訓練拠点、海外の有力研究者と日本国内の研究者を取り次ぐ国際連携拠点など様々な種類が考えられる。それぞれの機能に合わせて大学や公的研究機関に設置し、その上で、量子情報処理の教育・訓練プログラムの開発・提供、正確で積極的なアウトリーチ・科学広報活動、スピンアウトする量子スタートアップ企業の積極的支援など、多様な施策により、持続性あるネットワーク構築が求められる。

これらの研究開発プロジェクトや研究開発ネットワークの成功は、量子コンピューターコミュニティのプレーヤーの充実と、エコシステムの醸成にかかっている。計算機科学・物理・数学・電子工学に跨がった研究者・技術者のコミュニティは萌芽期であり、多分野連携・産学連携・技術レイヤー連携を可能とする研究開発・人材育成の拠点形成を念頭にした政府投資により、コミュニティ形成・エコシステム形成を強力に促進することが不可欠である。

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・国際会議における日本の存在感は薄い。第2次ブームでの出足は遅かったが、JST 戦略事業 (CREST・さきがけ・ERATO)、大型プロジェクト (Q-LEAP)、政府研究開発投資 (SIP) が開始された。しかし、官民投資規模は米中欧と比較して依然として桁落ち以下である。
	応用研究・開発	△	→	・産業化に向けた応用研究、製品開発には至る研究成果は顕著でない。NEC、NTT、日立製作所などには量子デバイス技術・量子光学技術の蓄積はあるが、計算機システムに至らない。 ・MDR、QunaSys、Jij などソフトウェア関連のスタートアップが登場したが、量・質ともに今後の発展が欲しい。
米国	基礎研究	◎	↗	・超伝導量子ビットでは UCSB の Martinis グループ (後に Google に移籍)、MIT、Yale 大学、UC パークレー、イオントラップでは Maryland 大学、Duke 大学、Harvard 大学がそれぞれ中心的存在である。量子情報分野では Caltech、MIT が中心的存在である。 ・国家量子イニシアティブにより、研究所の新設も予定されている。 ・IEEE Rebooting Computing Initiative などコンピューターサイエンス側も活発な活動が進む。
	応用研究・開発	◎	↗	・Google、IBM、Intel、Microsoft が研究を進める。応用研究だけでなく、基礎研究も行われている。 ・多様なスタートアップが登場し、Google や IBM などエコシステムが形成されつつある。
カナダ	基礎研究	○	↗	・「Seizing Canada's Moment」で ICT 優先テーマに量子コンピューティングが明記され、Waterloo 大学の Institute for Quantum Computing (IQC) に大規模な研究費支援がなされた。量子情報の基礎研究では同地区にあるペリメータ研究所も顕著な成果を上げている。
	応用研究・開発	○	↗	・ウォータールー地区は BlackBerry 創業者の Lazaridis による寄付で研究所が集積、「Quantum Valley」となりつつある。 ・西側のプリティッシュコロンビア州でも D-wave Systems、1QBit など量子アニーラー関係のスタートアップが活躍している。
欧州	基礎研究	○	↗	・多数の大学での量子情報科学の基礎研究の取り組みがある。EU Quantum Technology Flagship プログラムが始まり、量子技術に関する多数の国際連携チームが採択された。 ・オランダの TU Delft にある QuTech では大規模な研究開発が進められている。
	応用研究・開発	△	→	・企業による量子コンピューター研究開発で目立つものは少ない。
中国	基礎研究	○	↗	・「国民経済・社会発展第十三次五カ年計画」で量子コンピューターが重大科学技術項目に明記され、中国科学院 (CAS) による拠点形成が進む。
	応用研究・開発	△	↗	・CAS-Alibaba 量子計算実験室が設立され、量子コンピューターのクラウド提供を行っている。

(8) 参考文献

- 1) 科学技術振興機構研究開発戦略センター, 『(戦略プロポーザル) 革新的コンピューティング～計算ドメイン志向による基盤技術の創出～』, CRDS-FY2017-SP-02 (2018)
- 2) IEEE Rebooting Computing, <https://rebootingcomputing.ieee.org/>
- 3) National Academies of Sciences, Engineering, and Medicine, *Quantum Computing Progress and Prospects*, The National Academies Press (2018)
- 4) F. T. Chong, D. Franklin and M. Martonosi, Programming languages and compiler design for realistic quantum hardware, *Nature* 549, 180 (2017)

- 5) A. C.-C. Yao, Quantum circuit complexity, Proc. The 34th Annual IEEE Symposium on Foundations of Computer Science, 352 (1993)
- 6) 小柴健史, 藤井啓祐, 森前智行, 『観測に基づく量子計算』, コロナ社 (2017)
- 7) M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000)
- 8) K. Fujii, *Quantum Computation with Topological Codes, From Qubit to Topological Fault-Tolerance*, Springer (2015)
- 9) Quantum Algorithm Zoo, <https://math.nist.gov/quantum/zoo/>
- 10) 田淵豊, 杉山太香典, 中村泰信, 超伝導技術を用いた量子コンピュータの開発動向と展望, 電子情報通信学会誌, Vol. 101, No. 4, 400 (2018)
- 11) R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland and J. M. Martinis, Superconducting quantum circuits at the surface code threshold for fault tolerance, *Nature* 508, 500 (2014)
- 12) H. Bernien, S. Schwartz, A. Keesling, H. Levine, A. Omran, H. Pichler, S. Choi, A. S. Zibrov, M. Endres, M. Greiner, V. Vuletić and M. D. Lukin, Probing many-body dynamics on a 51-atom quantum simulator, *Nature* 551, 579 (2017)
- 13) A. W. Harrow and A. Montanaro, Quantum computational supremacy, *Nature* 549, 203 (2017)
- 14) Executive Office of the President of the United States National Science and Technology Council (NSTC), *National Strategic Overview for Quantum Information Science* (2018)
- 15) European Commission, *Quantum Manifesto* (2016)
- 16) 国務院, 『国家十三五国民経済・社会発展計画綱要』(2016)
- 17) Quantum Technologies Strategic Advisory Board, *National strategy for quantum technologies: A New Era for the UK* (2015)
- 18) Government of Canada, *Seizing Canada's Moment: Moving Forward in Science, Technology and Innovation* (2014)
- 19) Bundesregierung, *Hightech-Strategie* (2018)
- 20) 文部科学省 科学技術・学術審議会 量子科学技術委員会, 『量子科学技術 (光・量子技術) の新たな推進方策～我が国競争力の根源となりうる「量子」のポテンシャルを解き放つために～ 報告書 (平成 29 年 8 月 16 日発表)』(2017)
- 21) F. T. Chong, D. Franklin and M. Martonosi, Programming languages and compiler design for realistic quantum hardware, *Nature* 549, 180 (2017)
- 22) Mingsheng Ying 著, 川辺治之 訳, 『量子プログラミングの基礎』, 共立出版 (2017)
- 23) R. LaRose, Overview and comparison of gate level quantum software platforms, arXiv:1807.02500 (2018)
- 24) D. C. McKay, T. Alexander, L. Bello, M. J. Biercuk, L. Bishop, J. Chen, J. M. Chow, A. D. Córcoles, D. Egger, S. Filipp, J. Gomez, M. Hush, A. Javadi-Abhari, D. Moreda, P. Nation, B. Paulovicks, E. Winston, C. J. Wood, J. Wootton, J. M. Gambetta, Qiskit

- Backend Specifications for OpenQASM and OpenPulse Experiments, arXiv:1809.03452 (2018)
- 25) B. Valiron, N. J. Ross, P. Selinger, D. S. Alexander, J. M. Smith, Programming the Quantum Future, *Communications of the ACM*, Vol. 58, No. 8, 52 (2015)
 - 26) 寺井弘高, 丘偉, 山下太郎, 大規模量子計算に向けた超伝導量子回路の作製技術, *低温工学*, Vol. 53, No. 5, 295 (2018)
 - 27) ScaffCC, <https://github.com/epiqc/ScaffCC>
 - 28) N. C. Jones, R. Van Meter, A. G. Fowler, P. L. McMahon, J. Kim, T. D. Ladd, and Y. Yamamoto, Layered Architecture for Quantum Computing, *Phys. Rev. X* 2, 031007 (2012)
 - 29) R. Van Meter and C. Horsman, A Blueprint for Building a Quantum Computer, *Communications of the ACM*, Vol. 56, No. 10, 84 (2013)
 - 30) F. Chong, Introduction to Grand Challenges and Research Tools for Quantum Computing, IEEE MICRO51 Tutorials (2018)
 - 31) 蓮尾一郎, 星野直彦, 量子プログラミング言語, *情報処理* Vol. 55, No. 7, 710 (2014)
 - 32) 阿部 英介, 伊藤 公平, 固体量子情報デバイスの現状と将来展望 – 万能ディジタル量子コンピュータの実現に向けて, *応用物理*, Vol. 86, No. 6, 453 (2017)
 - 33) 今道貴司, 井床利生, ルディーレイモンド, 量子コンピューターを使ってみよう – QISKitを用いた量子プログラミングの紹介 –, *オペレーションズ・リサーチ* Vol. 63, No. 6, 350 (2018)
 - 34) A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow and J. M. Gambetta, Hardware-efficient variational quantum eigensolver for small molecules and quantum magnets, *Nature* 549, 242 (2017)
 - 35) J. S. Otterbach, R. Manenti, N. Alidoust, A. Bestwick, M. Block, B. Bloom, S. Caldwell, N. Didier, E. Schuyler Fried, S. Hong, P. Karalekas, C. B. Osborn, A. Papageorge, E. C. Peterson, G. Prawiroatmodjo, N. Rubin, Colm A. Ryan, D. Scarabelli, M. Scheer, E. A. Sete, P. Sivarajah, Robert S. Smith, A. Staley, N. Tezak, W. J. Zeng, A. Hudson, Blake R. Johnson, M. Reagor, M. P. da Silva, C. Rigetti, Unsupervised Machine Learning on a Hybrid Quantum Computer, arXiv:1712.05771 (2017)
 - 36) K. Mitarai, M. Negoro, M. Kitagawa, and K. Fujii, Quantum circuit learning, *Phys. Rev. A*, 98, 032309 (2018)
 - 37) IBM Qiskit Developer Challenge, <https://qe-awards.mybluemix.net/>
 - 38) 森前智行, 『量子計算理論 量子コンピュータの原理』, 森北出版 (2017)
 - 39) A. M. Dalzell, A. W. Harrow, D. E. Koh, R. L. La Placa, How many qubits are needed for quantum computational supremacy?, arXiv:1805.05224 (2018)
 - 40) IEEE Standards Association P7130 – Standard for Quantum Computing Definitions, <https://standards.ieee.org/project/7130.html>
 - 41) IEEE Rebooting Computing, An IEEE Framework for Metrics and Benchmarks of Quantum Computing (2018)
 - 42) T. F. Rønnow, Z. Wang, J. Job, S. Boixo, S. V. Isakov, D. Wecker, J. M. Martinis, D. A.

- Lidar, M. Troyer, Defining and Detecting Quantum Speedup, *Science* 345, 6195, 420 (2014)
- 43) R. Harris, Y. Sato, A. J. Berkley, M. Reis, F. Altomare, M. H. Amin, K. Boothby, P. Bunyk, C. Deng, C. Enderud, S. Huang, E. Hoskinson, M. W. Johnson, E. Ladizinsky, N. Ladizinsky, T. Lanting, R. Li, T. Medina, R. Molavi, R. Neufeld, T. Oh, I. Pavlov, I. Perminov, G. Poulin-Lamarre, C. Rich, A. Smirnov, L. Swenson, N. Tsai, M. Volkman, J. Whittaker, J. Yao, Phase transitions in a programmable quantum spin glass simulator, *Science* 361, 6398, 162 (2018)
- 44) H. Nishimori and K. Takeda, Exponential Enhancement of the Efficiency of Quantum Annealing by Non-Stoquastic Hamiltonians, *Front. ICT*, 17 (2017)
- 45) 科学技術振興機構研究開発戦略センター, 『(戦略プロポーザル) みんなの量子コンピューター～情報・数理・電子工学と拓く新しい量子アプリ～』, CRDS-FY2018-SP-04 (2018)
- 46) T. S. Metodi, A. I. Faruque, F. T. Chong, *Quantum Computing for Computer Architects*, Morgan & Claypool (2011)

2.4.3 データセンタースケール・コンピューティング

(1) 研究開発領域の定義

Google、Amazon、Facebook などの IT 巨大企業はサービスを提供するために巨大なデータセンターを運用している。数十万台あるいは数百万台のサーバーを設置し、それをつなぐネットワーク、ストレージなどが数百メートル四方の広さの建屋に設置されている。このような大規模データセンターにおいては、従来のラックスケールの考え方だけでは不十分である。物理的な制約も考えて、サーバー、ネットワーク、ストレージの配置や処理方式を最適化しなければならない。本研究開発領域においては、こういった大規模データセンターに向けた研究開発課題を俯瞰する。

(2) キーワード

データスケール・コンピューティング、メモリー・セントリック・コンピューティング、Hyper Converged Infrastructure、AI アクセラレータ、デジタルアニーラ、高速不揮発性メモリー、高速インターコネクト

(3) 研究開発領域の概要

[本領域の意義]

情報検索や EC サイト、SNS などのサービスがグローバルに拡大するとともに、スマートフォンとクラウドコンピューティングの融合によるさまざまなサービスの利活用、IoT を代表とする膨大なデータの取得と処理などによって、データセンターで処理するデータ量は近年ますます増加している。これまでのラックスケールでの計算実行から、データセンタースケールでの計算の実行へと移りつつある。また、膨大なデータを対象とした情報処理では、計算（プロセッシング）よりもデータの記憶・移動に要する時間がボトルネックとなる。そのため、プロセッサを中心とするコンピューティング（プロセッサ・セントリック・コンピューティング）だけでなく、メモリーを中心とするコンピューティング（メモリー・セントリック・コンピューティング、あるいはデータ・セントリック・コンピューティング）が必要になる。磁気メモリー（MRAM）、抵抗変化型メモリー（ReRAM）、相変化メモリー（PCRAM）といった高速な不揮発性メモリーや、光通信技術などの登場により、従来の Flash/HDD デバイスや電気通信と比較してデータを高速に転送・記憶することが可能になりつつある。このような、膨大な数のサーバー・メモリー・ストレージ・インターコネクトで構成されるデータセンターが今後のクラウドコンピューティングにおいて重要な役割を果たす。

[研究開発の動向]

電子計算機は 1949 年に実用的なプログラム蓄積方式の EDSAC (Electronic Delay Storage Automatic Calculator) が開発されてから約 70 年間で 10^{12} 倍という驚異的な性能向上を遂げてきた。これは、平均して約 1.5 年で 2 倍という指数関数的な向上であり、技術的には半導体の微細加工技術の向上が最も大きな要因であった。しかし、2000 年代に入るとチップあたりの消費電力の壁、動作周波数向上の壁、動作電圧低下の壁などにより、性能向上の陰りが見えてきた。すなわち、単純な微細化に頼ったムーアの法則の終焉である。

コンピューティングデバイスだけでなく、メモリーでも特徴的なデバイスの開発が進められている。2015年にIntelとMicronが共同でDRAMより大容量な128Gbitの3D-Xpointメモリーを発表¹⁾、2018年5月にはIntelがDDR4スロットに挿せる「Optane DC」不揮発性メモリーを発表した²⁾。SAPはこの大容量不揮発性メモリーを自社のインメモリーDB製品に適用し、大容量と不揮発性を生かしデータ処理能力と可用性の劇的な向上を目指している³⁾。これまでメモリー層はDRAMが利用されてきたが、DRAMの大容量化の鈍化によりDRAMとOptane DCメモリーなど複数のメモリーデバイスを組み合わせる取り組みが進んでいる。Samsungからアクセス時間が10μs以下の極めて高速であるが小容量なFlashメモリー技術⁴⁾と、それを採用したSSDが発表されている。一方で大容量化を目指したQLC-Flash⁵⁾が登場するなど、微細化による汎用品の性能・容量の向上から、次の時代に向けた目的特化の技術の開発が加速している。

これら特徴的なコンピューティングデバイスとメモリーデバイスを活用する新しいアーキテクチャの取り組みとして、HPEのThe machine⁶⁾が挙げられる。大容量な不揮発性メモリーを中心に、高速ネットワークで各種の特化型プロセッサと接続することで、データ移動を抑えたデータセントリックのコンピューティングを目指している。データセントリックの概念はビッグデータ処理に特化したソフト技術によりApache Hadoop⁷⁾でも一部実現されている。Hadoopでは、大量のデータを複数ノードで構成された分散ファイルシステムに格納し、極力データのあるノードで処理を行う。既存アーキテクチャをベースに、ストレージとコンピュータノードがネットワークで分断されることなく、データのあるところで処理するデータセントリックな構成となっている。また、従来は専用ハードで提供されていたネットワークやストレージ機能をソフトウェアで実現するSDx (Software Defined X) 化が進展し、汎用サーバー上のソフトウェアとして統合型基盤を実現できるようになってきた。事前にネットワーク機能やストレージ機能をインストールしておくことで、設置や増設時の設定作業を排したHyper Converged Infrastructure(HCI)⁸⁾が注目されている。HCIは簡単利用が注目され普及してきたが、HCIではローカルディスクを利用するため、データを仮想マシンの近傍に配置することで、データの移動を最小限に抑え、優れたパフォーマンスを実現するアーキテクチャとなっている。

既存の多くのデータセンターは仮想化基盤上で運用されるが、これは性能が同じである大量のコンピューティングリソースから、ユーザが求めるリソースを切り出し提供する技術である⁹⁾。ドメイン指向コンピューティングでは、様々なコンピューティングリソースやメモリーリソース中からアプリケーションに最適なハードを選択し再構成する技術が必要となる。Intelが進めているラックスケールデザイン¹⁰⁾は、サーバーを構成するプロセッサやメモリー、ストレージなどを分解し、サーバー単位ではなくラック単位でコンピューターを構築することにより、アプリに応じて最適な構成をとることが可能となっている。製品化の例として、HPEの「HPE Synergy」¹¹⁾が挙げられる。コンピューター、ストレージがリソースプール化されており、各ワークロードに合わせて再構成できる。いずれもラックスケールでの例であるが、データセンタースケールに拡張することでさらなるリソースの最適化が可能となる。

従来型アーキテクチャの性能向上が飽和する一方、処理すべきデータ量は爆発的に増加し続けており、2025年には175ZBに達すると予想されている¹²⁾。このままでは、従来型コンピューティングの処理能力を上回るのは明白であり、大量データの中から新たな知見を得るための

新しい情報処理技術の創造が課題となる。従来のアーキテクチャは数値処理に優れていたが、データセンターに集約された大量データから情報や知識を効率よく創出するデータセンタースケールのアーキテクチャへの進化が求められている。深層学習を始めとした AI 技術では、従来のように人がシステムを演繹的に設計・構築するのではなく、学習用データを使ってシステムの動作を帰納的に定義する。学習のためには大量のデータが必要であるため、高品質な大量データ活用技術が新しいサービスの源泉となる。

また、リアルタイム性を要求するシステムにおいては、データセンター側までデータを転送する時間が許容できず、エッジ側での深層学習処理などが必要な場合もあり、データセンター側とエッジ側の連携アーキテクチャが重要な課題である。

(4) 注目動向

[新展開・技術トピックス]

次世代メモリーの実用化とプログラミングモデルの整備

2015年にIntelとMicronが共同でDRAMより大容量な128Gbitの3D-Xpointメモリーを発表した。学会では各種の次世代不揮発性メモリーが議論されてきたが、3D-XPointは商用化された最初の大容量不揮発性メモリー技術である。ダイあたりの容量は128GbitとDRAMより1桁大きく、2015年当時のFlashメモリーに近い容量である。高速SSDとして製品化され、FlashメモリーベースのSSDより1桁高速な性能を実現している¹³⁾。また、2018年5月にはIntelがDDR4スロットに挿せる「Optane DC」不揮発性メモリーを発表し、主記憶としての不揮発性メモリーを実現した。従来、主記憶であるDRAMは揮発性であることを前提にプログラミングされており、主記憶が不揮発化することを想定していない。ストレージの業界団体であるStorage Networking Industry Association(SNIA)は、不揮発性メモリーに対するプログラミングモデルを標準化し、Persistent Memory Development Kit(PMDK)¹⁴⁾と呼ばれる不揮発性メモリーを活用するためのライブラリが開発されている。また、Hypervisor、OS、ファイルシステムでもバイトアクセス可能な不揮発性メモリーを活用する対応¹⁵⁾が進められ、新しい時代のメモリーデバイスの活用に向けて環境の開発が加速している。

Gen-Z consortium

本コンソーシアムは2016年10月に大手のコンピューティングやメモリー企業12社によって設立され、不揮発性メモリーやGPU、FPGAなどをメモリーセマンティックに接続する広帯域で低レイテンシーなインターコネクトの実現を目指している¹⁶⁾。2018年にはコア仕様1.0を公開、ベンダーがGenZ規格のインターコネクトの開発を可能にしている。多種多様な新しい不揮発性メモリーやコンピューティングデバイスに対応し、他のインターコネクトと比較してメモリーセマンティックで通信する上での特徴的な機能が盛り込まれている。不揮発性メモリーと様々なドメインに特化したコンピューティングデバイスをつなぎ、メモリーに格納されたデータを中心にした新しいアーキテクチャを実現する上で主要な構成要素である。

Open Compute Project (OCP)

OCPとは、2011年にFacebookの呼びかけにより発足したデータセンターのファシリティからサーバーに至るまでの管理仕様を公開したプロジェクト¹⁷⁾。現在は、MicrosoftとIntel

を加えた3社が牽引し、200社弱のベンダーが参画、データセンターの標準化を目指している。ハードウェア仕様の標準化からスタートし、2017年のSummitでは、ソフトウェアやファームウェアの標準化にも着手している。MicrosoftはProject Olympusというサーバー仕様を公開、データセンターの管理粒度をサーバーからラックにしようとしている。Intelは、自社のIntel Rack scale designを標準化すべくOCPに参画している。

【注目すべき国内外のプロジェクト】

日本ではAI応用などに向けた新しいコンピューティングの国家プロジェクトとして、2018年度からJST CREST「Society5.0を支える革新的コンピューティング技術」、JST さきがけ「革新的コンピューティング技術の開拓」、NEDO「高効率・高速処理を可能とするAIチップ・次世代コンピューティングの技術開発事業」が始まっている。しかし、カバーすべき領域がエッジ、データセンター、インターコネクットのハード・ソフトと広範であるため、例えば本研究開発領域であるデータセンター向けの研究開発が十分にカバーされているとは言い難く、より一層の強化が必要である。

米国においては、The National Computing Initiative(NSCI)が2015年の大統領令によって発足し、ハイ・パフォーマンス・コンピューティングでの米国のリーダーシップを実現しようとしている。NSCIは複数の省庁にまたがる統一的な戦略であり、産業、アカデミアの連携のもとに活動を進めている。National Science Foundation (NSF)においても、NSCI@NSFと題して、HPCの研究開発と配備に対してファンディングを行っている。Energy-Efficient Computing: from Devices to Architectures (E2CDA)というプログラムでは、材料からデバイス、コンピューティングアーキテクチャなどの研究に対して、2016年から18年に合計で2千2百万ドル、Scalable Parallelism in the Extreme (SPX)においても2千万ドルの研究資金を提供している。また、Petascale Computing Resource Allocations (PRAC)においては、実際にスーパーコンピューティング環境を構築するために、2013年から2018年までに3億3千万ドルが投資されている。

これまでコンピューティングの性能向上を支えてきたムーアの法則の終焉を迎え、コンピューティングを根底からすべて考え直そうという動きがIEEEのRebooting Computing Initiativeである。材料、デバイス、システム、アーキテクチャ、言語など多くの領域の専門家が集い、コンピューティングの将来を模索している。

欧州においてはHORIZON2020において、Advanced Computingというトピックを設定し、2014年から研究提案を募集し、現在30以上のプログラムが実行されている。低電力プロセッサ、フォグコンピューティング、ディープラーニングの学習アルゴリズムなど多岐にわたる研究が推進されている。2015年から2017年の間に開始されたプロジェクトへの投資金額は総額1億5千万ユーロに達する。

(5) 科学技術的課題

AIアクセラレータ、高速な不揮発性メモリー、高速インターコネクタなど、AIを使ったリアルタイム処理などを差別化するハードウェア技術の研究を強力に推進することは当然、必要である。ただし、こうしたハードウェアのキラー技術の能力を最大限に発揮させるためには、個別のハードウェアの研究開発だけでは不十分であり、ハードウェアを融合したサーバー・ス

トレージを構築するための、OS、デバイスドライバ、分散処理・データベース等のミドルウェアなど、ハードウェア・ソフトウェアを統合・全体最適化したコンピューティング技術の研究開発が必須になる。ハードウェア・ソフトウェアの統合は1つの企業、単独の研究機関・大学では行うことは難しく、分野のレイヤをまたいだ複数の産学の連携が必要になる。

(6) その他の課題

(5)で記載のように、ハードウェア・ソフトウェアを統合・全体最適化したコンピューティング技術の研究開発では、分野のレイヤをまたいだ複数の産学の連携が必要になる。また、日本の産業界の状況に鑑みても、遠い将来の技術・コアとなる事業以外の技術の研究開発に投資を行うことが難しくなっている。いわゆる中央研究所が減ってきていることはその一つの象徴ではないか。そのため、日本企業が将来にわたって競争力を保つためには、外部の研究機関・大学を「基礎研究や異分野融合のための研究開発リソース」として活用することが極めて重要になると考えられる。

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	↘	・一部の有力な研究者がトップカンファレンスで発表しているが、アーキテクチャ分野での存在感は低い。
	応用研究・開発	○	↗	・業務のデジタル化が進み、自動車など強い業種に特化したデータセンターの研究開発が進められている。
米国	基礎研究	◎	→	・産業界と大学が協力し、アーキテクチャのトップカンファレンスでの発表件数は首位。コンピューティングの主要な部品ベンダーを擁しており圧倒的。
	応用研究・開発	◎	→	・Amazon、Google、Facebook、Microsoftなどメガデータセンタを運用するプラットフォームが主導。最新開発成果は自社で利用した後に発表するほどの開発力を持ち、自社サービスを強化するハード、ソフトを強化。
欧州	基礎研究	○	→	・SAPのファウンダーが創設したHPIや、Tableauに買収されたHyperを開発したミュンヘン工大など、DB分野では数多くの成果をトップカンファレンスで発表。
	応用研究・開発	○	→	・Horizon Europeにおいて、Cloud ComputingのWork Programmeを実行するなど、具体的な応用に向けた研究開発が進められている。
中国	基礎研究	○	→	・スーパーコンピューターではトップクラスの性能を実現している。
	応用研究・開発	◎	↗	・Baiduは2018年にAIチップである「Kunlun」、Alibabaは「Ali-NPU」を開発するなどAI分野で攻勢。データセンターの規模でも、AlibabaクラウドはAWS、AZUREに次ぐ第3位のシェア。
韓国	基礎研究	○	→	・Samsungなどメモリーベンダの存在感が大きく、大学でもメモリーにかかわる研究テーマが多い。メモリー技術に関しては、トップカンファレンスで発表する力を持つ。
	応用研究・開発	○	→	・電子政府の普及など、実用化が進んでいる。

(8) 参考文献

- 1) Intel News Release July 28, 2015, Intel and Micron Produce Breakthrough Memory Technology, <https://newsroom.intel.com/news-releases/intel-and-micron-produce-breakthrough-memory-technology/#gs.gq890Fs>.
- 2) Intel News Release May 30, 2018, “Reimagining the Data Center Memory and Storage Hierarchy”, <https://newsroom.intel.com/editorials/re-architecting-data-center-memory-storage-hierarchy/#gs.234zB98>.
- 3) SAP HANA Blog, “Continuous and Customer-Driven Innovation with SAP HANA”,

- <https://blogs.saphana.com/2018/06/05/continuous-and-customer-driven-innovation-with-sap-hana/>.
- 4) Wooseong Cheong et al. “A Flash Memory Controller for 15us Ultra-Low-Latency SSD Using High-Speed 3D NAND Flash with 3us Read Time” International Solid-State Circuits Conference (ISSCC), 2018.
 - 5) 東芝メモリプレスリリース 2017年6月28日、世界初、QLC技術を用いた3次元フラッシュメモリ「BiCS FLASH™」の開発について、<https://business.toshiba-memory.com/ja-jp/company/news/news-topics/2017/06/memory-20170628-1.html>.
 - 6) Hewlett Packard Enterprise Press release May 16, 2017, “HPE Unveils Computer Built for the Era of Big Data” , <https://news.hpe.com/a-new-computer-built-for-the-big-data-era/>.
 - 7) Apache Hadoop, <https://hadoop.apache.org/>
 - 8) IDC Japan, 国内コンバージドシステム市場予測を発表、<https://www.idcjapan.co.jp/Press/Current/20180820Apr.html>.
 - 9) Takashi Miyoshi, Kazuichi Oe, Jun Tanaka, Tsuyoshi Yamamoto and Hiroyuki Yamashima, New System Architecture for Next-Generation Green Data Centers: Mangrove, FUJITSU SCIENTIFIC & TECHNICAL JOURNAL Vol.48, No.2.
 - 10) Intel Rack Scale Design, <https://www.intel.com/content/www/us/en/architecture-and-technology/rack-scale-design-overview.html>.
 - 11) Hewlett Packard Enterprise, HPE Synergy, <https://www.hpe.com/jp/ja/integrated-systems/synergy.html>.
 - 12) David Reinsel, John Gantz and John Rydning, The Digitization of the World From Edge to Core, IDC White Paper, 2018.
 - 13) F.T. Hady, A. Foong, B. Veal, and D. Williams, “Platform Storage Performance With 3D XPoint Technology,” Proceedings of the IEEE, vol.105, no.9, pp.1822–1833, 2017.
 - 14) Andy Rudoff, Persistent Memory Programming: The Current State and Future Direction, SNIA Persistent Memory Summit 2019.
 - 15) Mark Carlson, Persistent Memory what developers need to know, SNIA Storage Developer Conference (SDC), 2018.
 - 16) GEN-Z, <https://genzconsortium.org/>.
 - 17) Open Compute Project, <https://www.opencompute.org/>

2.4.4 ビッグデータ処理基盤技術

（1）研究開発領域の定義

本領域は、大量な台数の計算機あるいはハイエンドな計算機を効果的に利用することで、大規模なデータ（ビッグデータ）に対する分析処理を効率的に実行する基盤的ソフトウェア技術を確立する領域である。主要要素技術は分散並列型の大規模データ分析処理であり、分析処理の種類はデータベース検索・機械学習・データマイニングが対象である。

（2）キーワード

データベース、機械学習、データマイニング、並列分散データ処理、最適化、分類、クラスタリング、クラウドコンピューティング

（3）研究開発領域の概要

【本領域の意義】

Data is the new oil（データは新しい石油である）といわれるように、ビッグデータを分析することで隠れた知識やルールを発見して、社会的あるいは経済的なインパクトを生み出すことが期待されている。先端的な分析処理に関する応用として、コンピュータ囲碁、Google や NICT などが取り組んでいる翻訳技術、自動運転や早期がんの診断支援¹⁾における映像・画像認識などが挙げられる。これらの応用例では共通して、大量のビッグデータを活用して人間の能力に近い情報処理の実現を目指している。一方、ペタバイトスケールの大規模データを扱う応用として、NTT ドコモが運用するモバイル空間統計（ドコモの携帯電話ネットワークのしくみを使用して作成される人口の統計情報）、国立天文台における観測データの画像解析、Amazon に代表されるクラウド環境を利用した多様なサービスが挙げられる。

市場調査会社の IDC Japan の 2018 年 8 月の報告²⁾によれば、2017 年の国内ビッグデータテクノロジー／サービス市場は、前年比 8.9% 増の高い成長率を維持し、市場規模は 8848 億 8900 万円となったとされている。更に、今後の予測として 2022 年の市場規模は 1 兆 5617 億 3100 万円に達し、年間平均成長率（CAGR：Compound Annual Growth Rate）は 121% になると報告されている。このようなビッグデータテクノロジー／サービス市場を牽引するのは、大規模データを対象としたデータベース検索・機械学習・データマイニングなどの技術である。

【研究開発の動向】

ビッグデータ処理の基盤システムに関する技術は、分析処理の種類に応じて、大規模データを管理するデータベース系の技術と、高度な分析を行う機械学習系の技術に分類することができる。

データベース系のクラウド技術

クラウド環境におけるデータベースの役割は、大規模データに対して、大量のクエリを高スループット・低レスポンス時間で処理することにある。代表的なシステムとして、小規模のハイエンドな計算機を用いる分散データベース管理システム（分散 DBMS）の技術と、1000 台を超える大量のコモディティ計算機を用いる NoSQL および Spark/MapReduce に代表される

分散処理システムがある。前者の分散 DBMS については Oracle、IBM、Microsoft などのデータベース製品や SAP の HANA に代表される主記憶型の DBMS が代表的である。後者については、Google がクラウドサービスとして提供している SQL エンジンの BigQuery、Amazon が提供する SQL エンジンの Redshift、NoSQL エンジンの DynamoDB、分散処理エンジンの Elastic MapReduce、そして Microsoft が提供する NoSQL エンジン Azure Cosmos DB 等が代表的である。

研究の動向として、1) 不揮発性メモリ・メニーコア・高速ネットワークボードなどの最新ハードウェアを活用した分散並列 DBMS の研究、2) データベースに対するアクセスパターンを分析予測することで高速な処理を実現するワークロード予測技術、3) クラウドにおける大量なクエリを高速に処理するためのインデックス選択技術や最適な実行プラン選択するクエリ最適化技術、4) 高速なデータ書き込みと分析処理を両立することでリアルタイムな分析を実現する HTAP (Hybrid transaction/analytical processing) 技術、5) 機械学習などの高度な分析応用とデータベース処理を融合した横断的最適化技術、6) 大規模データを分析する事前処理としてデータクリーニングを効率化する技術 (data wrangling) などが挙げられる。1 に関してはハードウェアベンダと大学の連携で研究が進められることが多く、2 と 4 に関しては企業が提供する実際のアクセスパターンを分析することで大学が研究を行うことが多い。3 に関するクラウド環境におけるデータ処理エンジンとしては、Google、Microsoft、Amazon、Facebook、Twitter などの Web 系の企業が先導しており、各社の専用の用途に応じて開発が進められている。5 と 6 は主に大学を中心に研究が進められている。

機械学習系のクラウド技術

クラウドにおける機械学習の実行環境は進化が目覚ましい。代表的なシステムとして、Google では画像認識、音声認識、多言語翻訳などのサービス (Google Cloud Machine Learning Engine) を実現する基盤システムとして深層学習の基盤技術 (TensorFlow) の開発を進めている。同様に、Microsoft でも画像認識、音声認識、検索エンジン、対話システムを提供する Microsoft Azure Cognitive Services の開発を進めている。IBM では Watson API を利用して画像認識、音声認識、自動翻訳などの機能を提供している。日本では、PFN が画像解析や物体検出技術に注力しており分散深層学習フレームワーク ChainerMN および画像認識フレームワーク ChainerCV を公開している。また、NTT ドコモは対話 AI を実現する API として、自然対話、トレンド抽出、音声認識などの機能を提供している。このほかにも、Keras や PyTorch、Caffe などさまざまな機械学習フレームワークがクラウドで提供されている。使用する言語やインストールの仕方、学習速度、処理の柔軟性、使いやすさなどに特徴があり、利用に当たっては適切なものを選択する必要がある。また、リアルタイム性を要する応用システムにおいては、機械学習系の処理をエッジ側で処理する必要があり、学習モデルの小型化、高速化、およびクラウド側との連携アーキテクチャが課題である。

国際動向

日本では、文科省の人工知能 (AI) 研究拠点として理化学研究所 AIP センター、経産省では産業技術総合研究所人工知能研究センター、総務省では情報通信研究機構脳情報通信融合研究センターが設立されており、ビッグデータ・AI 向けのプロジェクトに重点化した戦略を国

が主導している。また、AI 向けのクラウド環境として、2018 年 8 月から産業技術総合研究所が研究者に AI 橋渡しクラウド（AI Bridging Cloud Infrastructure、ABCI）のサービス提供を開始している。ABCI は理論ピーク性能が半精度で 550PFLOPS、倍精度で 37PFLOPS のスパコンによって実現されており、2018 年 11 月のスパコンの速度性能ランキング（TOP500）で世界 5 位に位置している。一方、企業の取り組みにおいては、2020 年の東京オリンピックを見据えて、自動車の自動運転・人流制御による渋滞解消・スポーツにおけるトレーニングや戦術の AI 導入などの取り組みが通信、メーカ、スタートアップなどの企業を中心に進められている。

米国では、Google、Amazon、Microsoft、IBM などのクラウド事業を手掛ける企業が GPU を利用できる深層学習向けのクラウドサービスを提供するとともに、簡単に AI を利用した応用プログラムを開発するための API の提供を行っている。代表的な企業である Google を例にとると、大規模な計算機環境を簡易に利用するためのコンテナ技術（Kubernetes）を開発し OSS として公開して世界での普及を進めており、ビッグデータの管理に関しては自社の分散データベース管理システムである F1 および Spanner の開発を進めている。また、機械学習に関しては開発環境である TensorFlow のソースコードを公開するとともに、機械学習に特化した Google の自社開発プロセッサ TPU を Google のクラウド環境で利用できるサービスを開始している。画像認識、音声認識、多言語翻訳などの AI 応用を簡単に開発するための API を提供している（Google Cloud Machine Learning Engine）。

EU におけるビッグデータに関する主な取組としては、Horizon2020（2014 年から 7 年間の計画で総額 770 億ユーロを投じる計画）において、ビッグデータの管理、研究のインフラの整備、データのオープンアクセスが進められている。AI・ビッグデータに対する競争力は EU 各国で状況が異なっているが、ドイツ・フランス・スイスが活躍している。企業の例としては、主記憶型 DBMS をコア技術とする SAP 社では、SAP Cloud Platform というクラウドサービスを提供しており、また大学ではミュンヘン工科大学が Google を含めて多くの企業と連携しており、スタートアップも輩出している。フランスではスタートアップが多く生まれしており、またフランス原子力庁（CEA; Commissariat à l'énergie atomique et aux énergies alternatives）では IoT 応用を対象としたシステムおよびクラウド開発を進めている。

中国では、企業としては Alibaba が商業的に成功しており（2018 年 10 月の株式時価総額世界ランキングにおいて世界 8 位）、米国の Amazon と同様に E コマースを運用するバックエンドのシステム向けの独自の大規模分散システムを開発し運用している。研究領域に関しては、マイクロソフトリサーチアジア（対話システム、コンピュータビジョン、検索システム等の研究）や IBM などの企業が活躍している。

韓国では、AI・ビッグデータに対して国家予算が多く投資されていると共に、Samsung などの企業において AI のスキルを有する人材の育成に取り組んでいる。

（４）注目動向

最新ハードを活用した並列分散データベースの高速化

クラウド環境で大規模データを分散並列処理するプロジェクトとしては UCB 発の Apache Spark³⁾ が著名であり、既に巨大なコミュニティに成長し世界的に普及している。分析処理方法も SQL、グラフ処理、機械学習と広範囲で豊富なライブラリ群を提供しており、多様な応

用に適用可能である。Spark ではメニーコアなどの最新ハードウェアを活用していないためハイエンド向きの計算機環境には適さない問題があったが、パーデュー大の Flare プロジェクト⁴⁾では Spark の足回りを Java から C 言語に変更し、メニーコアの代表的な NUMA(Non-Uniform Memory Access) 環境を活用するため OpenMP を用いたクエリ実行エンジンを研究している。また、データベース管理システムで最新ハードを活用する代表例としてミュンヘン工科大学の Hyper project⁵⁾では、メニーコアを活用し高速なトランザクション処理および分析処理を両立するメインメモリーのデータベースエンジンの研究を行っており、2016年に BI サービスの Tableau 社に買収されている。

データベース処理と機械学習の連携による処理の最適化

世の中の大半のデータはデータベースに格納されているため、データベースからデータを取り出して機械学習を適用する必要がある。従来は、データベースの最適化と機械学習の最適化が局所的に独立に行われていたため、システム全体としての最適化が行われていなかった。この問題に対して、UCSD の Triptych project⁶⁾では、機械学習におけるデータ処理に関する情報をデータベース側に伝えることによって、システム全体としての最適化を行う研究に取り組んでおり、特徴量抽出のような線形的な学習から深層学習のような非線形な学習にわたる最適化の技術の研究に取り組んでいる。同様の文脈で、データベースに格納された複数のテーブルを1つに結合することなく学習する技術として Markov Logic があり、ワシントン大学の Pedro Domingos 教授が該当分野の第一人者である。

データクリーニングの自動化

機械学習やデータマイニングの処理においては、アルゴリズムにデータを入力する前にデータのフォーマットを加工したりノイズを除去したりするデータクリーニングの操作が必要であり、データクリーニングの操作は分析工程の大半を占めることが知られている。しかし、データクリーニングの処理は一般化することが難しいため、データ分析者が多くの時間を費やして手動で行わざるを得ないという問題があった。この問題を解消する手段として、近年 Data Wrangling という技術が注目されておりオライリーの書籍なども発刊されている。Data Wrangling に関する近年の取り組みとして UCB の DataWrangler プロジェクト⁷⁾があり、ユーザが GUI からデータを操作することで期待されるクリーニング操作を推定して、自動的にプログラムを生成するツールを開発している。本研究プロジェクトから Trifacta 社がスタートアップとして起業し、ツールの商用化に取り組んでいる。

発見的データ分析

ビッグデータを扱う現在、データの多様性が増しており、膨大な情報の中から仮説を立案して検証を行う従来型の仮説検証型のデータ分析が困難になりつつある。この問題に対して、発見的データ分析の技術がある。発見的データ分析の起源は古く 1977年に John Tukey が提唱した detective work に遡る。代表的な研究として、イリノイ大の zenvisage project⁸⁾やワシントン大の HypDB project⁹⁾が挙げられる。特に HypDB はベイズネットワークとデータ分析を融合した技術であり、隠れた因果関係を探索して見つけるという特徴を持つ分析技術である。

機械学習の生産性向上

機械学習に関しては研究が多岐に渡るとともに、急速なスピードで研究が進んでいる状況にある。その中でもクラウド環境で利用されてきている技術として、多様な機械学習アルゴリズムの自動選択と自動パラメータチューニングを行う Automated Machine Learning (AutoML) があり、2013年の Auto-weka の頃から注目され、現在では多くのプロジェクトが存在する。代表例の1つとして Google Cloud AutoML¹⁰⁾ はクラウド環境において利用することが可能になってきている。Google Cloud AutoML では、画像認識、テキスト分類、翻訳のサービスを提供しており、教師データを入力するだけで、機械学習の非専門家であってもカスタムの学習モデルを構築することが可能である。同様なサービスとして、Apple では Create ML¹¹⁾ というツールキットを提供しており、画像分類とテキスト分類に関して GUI 操作でモデル学習することができ、簡単にスマートフォンアプリに組み込んで利用することが可能である。

量子計算を用いた DBMS の高速化

近年、量子コンピュータが注目されており、Google、IBM、D-wave、NII と NTT の共同研究などの取り組みがある。この量子計算の仕組みを、DBMS の処理の最適化問題に適用するという研究がスイス連邦工科大学ローザンヌ校で取り組まれている¹²⁾。この研究では、DBMS の最適化を D-wave 社の計算機で実行している。また、NTT では、量子計算のクラウドサービス QNNcloud¹³⁾ の提供の準備を進めており、量子計算を一般ユーザでも利用可能な時代になりつつある。

(5) 科学技術的課題

データベース系のクラウド技術について

ビッグデータの特徴は Volume (大規模)、Velocity (高い更新頻度)、Variety (多様) の 3V と言われるが、すべてを満たすデータベースエンジンは完成しておらず、中長期的に見て取り組むべき重要課題と言える。

現在の研究開発では、3V の任意の1つだけ高いレベルで実現するか、あるいは2つの両立を目指す研究が進められている。例えば、時々刻々と変化する大規模データを瞬時に捉えて分析する技術は、Volume と Velocity を両立する一例であり、これはデータベースにおけるトランザクション処理 (OLTP) と分析処理 (OLAP) を両立するという重要な技術課題である (前述の Hyper project はこの範疇に入る)。また、前述の発見的データ分析は、有益な知識を発見するため膨大で多様な属性群の中から適切な属性を探索する技術であり、Volume と Variety を両立する一例である。異なるスキーマを有する大量なデータベース群をデータ統合して参照利用するケースも Volume と Variety を両立する一例と言える。この例を更に発展させて、時々刻々と変化するデータベースの更新を他のデータベースに即時に伝播して更新を反映する技術は3つのVを全て両立する一例であり、チャレンジ性が高い課題である。

機械学習系のクラウド技術について

現在の大きな課題として、学習モデルの再利用の促進とそれに必要となる要素技術の研究を挙げる。現在、全世界的に機械学習のアルゴリズム研究が急速に進んでおり教師データの公開

も一部進んでいるが、学習モデルの再利用がされることが少ないため、全世界で同じ評価実験を行って稼動と電力を無駄に消費している状況にある。また、学習モデルを再利用せずにゼロから学習を行うことは、人間で例えると新生児の状態から学習を行うことに相当するため、無駄が大きいことは明らかである。このため、今後は学習モデルの再利用を進めるための共有化のフレームワークと要素技術開発が必要である。具体的には、共有化された膨大な学習モデル集合の中から適用先に適した学習モデルを選別するデータベースの技術、探索した学習モデルを転用するための転移学習の技術（これは現在でも盛んに行われている）、転移学習後の再学習において破壊的忘却を避ける技術、既存の学習モデルの一部を切り出して再利用する、あるいは複数のモデルを合成して再利用するといった学習モデル変換の技術の開発が重要な課題になると考えられる。

（6）その他の課題

本研究開発領域に限らないが、大学における研究体制の大きな問題は特任雇用の不安定さである。企業に就職すれば充実した退職金制度と年金が受給されるのに対して、特任教員には制度が充実していないため、優秀な学生が大学へ就職することのハードルになっている。

更に、研究開発を推進する上での日本社会における問題として、博士進学希望者が少ないこと、および産学連携による大学から企業への技術移転が少ないことが挙げられる。両方とも多様な原因と対策が考えられ、大学の教育の在り方も再考が必要であるが、大きな原因の一つは人材の流動性が低いことであると考えられる。社会流動性が低いため、博士のような資格の重要性が高くなく、博士号の取得が学生へのモチベーションになりにくい。一方、企業側から見た場合、突出した能力の学生を採用するよりも、早い段階で企業文化に馴染んだ方が望ましいため、博士よりも修士を採用する傾向にある。また、社会流動性が低いため、特に企業から大学あるはその逆の方向に転職する人材が極めて少なく、その結果、産学連携にプラスに働かない状況にあると考えられる。現実的には人材の移動は障壁が高いことから、近年は企業や大学でクロスアポイントメントを導入する兆しが見えてきている。しかし、依然として企業と大学間のクロスアポイントメントの利用はごく少数である。

日本人が世界で活躍するような施策も必要である。義務教育期間で言えば、実用的な英語教育が必要であり、最も効果がある施策としては大学入試の英語を実用的な英語試験に変更する方法が考えられる。博士卒業生に関して言えば、日本の企業では修士と博士とで給与差が大きいため、海外企業に就職するモチベーションが大きいことはプラスの要因と捉えることはできる。大学の教員に関しては、日本ではサバティカル制度の活用が進んでおらず対策が必要である。

本領域特有の問題点としては、データベース系および機械学習系のクラウド技術に関して、企業および大学共に米国が市場的にも技術的にも先行していることである。Eコマースなどの応用分野の事業領域では拮抗しているが、クラウド事業¹⁴⁾に関してはAmazonをはじめとする海外クラウド企業が日本市場の7割を超すシェアを占めてしまっている。また、クラウドの運用コストは電力費が多くを占めるため、低コストな電力が提供される地域のクラウドサービスが有利な傾向にある。クラウド事業が本研究開発領域の出口として重要であるとともに、事業から得られる課題こそが新たな研究開発を駆動する力となることを考慮すると、今後の国家的な施策として、日本企業によるクラウド事業と技術開発を支援する必要があると考えられる。

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・データベース分野での最難関会議の SIGMOD2017 では、大規模データの高速分析処理に関して、過去最高レベルの4人の日本人発表があった。クラウド系の基盤技術に関する発表は全体で増加傾向にあるが、一方、日本からの発表は減少している。機械学習系の最難関会議では、日本の大学および企業からコンスタントに発表されている。
	応用研究・開発	○	→	・Apache Spark のコミットに新たに2名が輩出され合計で4名(67名中)の日本人がコミット登録され、ビッグデータ処理基盤のOSSへの日本からの貢献が伸びている。 ・Preferred Networks が開発する深層学習エンジン Chainer は市場ランキングが下降気みである、 ・日本の電機メーカ、自動車メーカ、研究機関等が大規模データの活用と人工知能を活用した応用に精力的に取り組んでいる。
米国	基礎研究	◎	→	・米国の大学・企業における基礎研究レベルは高く、データベース系および機械学習系の両面で世界をリードしており、特にデータベース分野での最難関会議の約6割は米国からの発表である。
	応用研究・開発	◎	→	・分散処理基盤技術の取り組みについては、Web系の企業がOSS開発を先導しており米国が圧倒している。OSS開発コミュニティでは大学との連携が強い。Logicblox や TigerGraph など大規模データ分析のスタートアップ企業も多い。Spark コミュニティは機械学習系の機能強化に取り組んでいる。
欧州	基礎研究	◎	→	・不揮発性メモリー・メモリーコア・高速ネットワーク・GPUやFPGAなどの最新ハードウェアを活用したDBMSの研究開発が強い。Hyper は Tableau 社に買収されており、産学連携が円滑に進んでいる。
	応用研究・開発	○	→	・SAPのHANAなどのカラム指向で主記憶型のDBMSやストリームデータ処理エンジンの取り組みが目立っている。
中国	基礎研究	○	→	・大学が中心となって基礎研究において多く成果を挙げている。難関国際会議への採録も米国・欧州に次いで3番目に多い。アルゴリズム系の研究が中心であるが、クラウド系の基盤技術の研究が増加しつつある。 ・現地の優秀な学生を囲い込むため、外資研究機関の現地法人化が進んでおり、Microsoft では、対話エンジンの研究を中心的に取り組んでいる。
	応用研究・開発	◎	→	・Alibaba が商業的に成功しており(2018年の世界時価総額において世界8位)、Eコマースを運用するバックエンドのシステム向けの独自の大規模分散システムを開発し運用している。 ・中国全体としてスタートアップ企業が好調である。例えば、大規模データを分析するためのシステムに関するスタートアップ企業 PingCAP は、高速DBMSのOSS製品を軸として事業化を成功させている。
韓国	基礎研究	○	→	・最新ハードウェアを利用したDBMSの高速化などの高速DBMSの取り組みや、グラフエンジンの取り組みなどが目立っている。
	応用研究・開発	△	→	・SAPは韓国に支店を構え、韓国の大学と共同研究を行い、SAP HANA DBMSの高速化に取り組んでいる。また、サムソンは大学と連携することで、AI教育に力を入れて始めている。

(8) 参考文献

- 1) AIで早期がん領域の高精度検出に成功 早期発見・領域検出で早期治療に大きく貢献
https://www.ncc.go.jp/jp/information/pr_release/2018/0721/index.html
- 2) IDC、国内BDAテクノロジー／サービス市場予測を発表、<https://www.idcjapan.co.jp/Press/Current/20180827Apr.html>
- 3) Apache Spark, Lightning-fast unified analytics engine, <https://spark.apache.org/>
- 4) FLARE, Scale up Apache Spark with Native Compilation and set your Data on Fire!, <https://flaredata.github.io/>
- 5) HyPer – A Hybrid OLTP&OLAP High Performance DBMS, <https://hyper-db.de/>
- 6) Project Triptych, <https://adalabucsd.github.io/triptych.html>
- 7) DataWrangler, <http://vis.stanford.edu/wrangler/>

- 8) zenvisage, A System for Effortless Visual Exploration of Large Datasets, <http://zenvisage.github.io/>
- 9) HypDB, Bias in OLAP Queries: Detection, Explanation, and Removal, <http://db.cs.washington.edu/projects/hypdb/>
- 10) Cloud AutoML, <https://cloud.google.com/automl/>
- 11) Create ML, Create machine learning models for use in your app., <https://developer.apple.com/documentation/createml>
- 12) Multiple Query Optimization on the D-Wave 2X Adiabatic Quantum Computer, PVLDB, 2016
- 13) QNNcloud, <https://qnncloud.com/index-jp.html>
- 14) MMRI、国内クラウド市場は 2019 年度に 2 兆円へ成長、<https://www.m2ri.jp/news/detail.html?id=37>

2.4.5 サービスプラットフォーム

(1) 研究開発領域の簡潔な説明

新しいコンピューティングメカニズムやネットワークエッジにおけるコンピューティングを実現する IoT/CPS デバイスによって生成されるデータを活用し、コンピューティングサービスを実現するプラットフォームとなるのがサービスプラットフォームである。サービスプラットフォームはサービスの受益者のコミュニティを形成し、サービス提供者をマッチングして相互の価値交換を行う取引を円滑にする。サービスプラットフォームは巨大なので、社会システムへの影響が大きい。

(2) キーワード

サービスプラットフォーム、5G、エッジコンピューティング、限界費用ゼロ

(3) 研究開発領域の概要

[本領域の意義]

サービスプラットフォームはサービスの提供者と消費者、プラットフォームの3アクターモデルである。サービスや物品のマーケットプレイス、ペイメントサービス、SNS やゲームなどのサービス交換型のプラットフォームと、YouTube のようなデジタルコンテンツ配信やアプリケーション開発を行う SFDC(Salesforce dot com) や Android/GooglePlay などのようなメーカー型のプラットフォームがある。マッチアップによる取扱手数料やゲームアイテムの販売などの有償サービスと、広告宣伝費に転嫁するフリーミアムのビジネスモデルが混在している。

これまでのアプリケーションソフトウェアの設計は商品検索、受発注処理、ポイント計算などの機能設計が中心だった。サービスプラットフォームのアプリケーションソフトウェアの設計で重要なのはユーザーのコンテキストを理解しプラットフォームへの帰属を拘束する戦略を実装することである¹⁾。機能を提供するソフトウェアは、コピーや模倣を通じてコモディティ化しやすく、同じような機能を利用する利用者が増えるほど機能の価値が下がってしまう。最終的には機能モジュールはオープンソースによるライセンス解放という道を辿ることも多い。一方、サービスプラットフォームには、利用者が増えれば増えるほど他の利用者の利便性も向上するというネットワーク効果があり、この効果はコピーされにくい。サービス提供者と消費者の共創が引き起こされ、つねにより良いサービスがプラットフォームに供給される循環が、両者の価値交換を円滑にする。また、旧来の冗長なプロセスがバイパスされるなどコア取引のフリクションを減らすことで利用者を誘引する。比較的スケールの大きなビジネスを実装する場合、サービスを企画する提供者と消費者の間でサービスの質や内容を直接調整することは難しいが、サービスプラットフォームはユーザーの性向、動向を把握しサービス提供者に対応を促して調整問題を解決することで、サービスプラットフォームへの帰属を拘束する²⁾。

ネットワーク効果を引き起こしプラットフォームに参加者を滞在させるためには、ユーザーの性向動向を詳細に知るデジタルマーケティングの手法が欠かせない。最新の WEB アプリケーションはユーザーのブラウザ上での行動を監視・収集してパーソナルプロファイルデータを作成する³⁾。

[研究開発の動向]

サービスプラットフォームは多くの人々を引きつけることによってその存在価値が維持される。したがって、サービスプラットフォームの提供する経済性や多様性、利便性も重要であるが、ユーザーにとっての信頼性がプラットフォームを選定する際の重要なファクターになる。サービスの継続性や可用性などの信頼性はすでに多くの研究開発がなされているが、ここではその内容の信頼性、信頼を保証するネットワークに関わる動向について述べる。

内容の信頼性については、機械学習におけるバイアスが問題になることがある。サービスプラットフォームの収集するデータには多くのバイアスが含まれる。Google 写真検索で” Grandmother” を検索すると、米国の人種的な人口構成に反してその多くは幸せそうに笑う白人女性である。データ収集時の現実社会とのずれは、人種バイアスであるとともにシェアされるシーンが幸せなシーンに偏りやすいという誘因も働いている。こうした記録のバイアスは実行時のデータが学習に利用されると増幅し、共振しやすい。さらにバイアスはデータだけではなくアルゴリズムにも潜んでいる。機械学習をバックエンドにした判断システムは特定の KPI に対して最適化する傾向にあり、その意図が政治的なものであろうと、単なる製品の広告であらうと関係なく、ただ「サイトの滞在時間を長くするように」というようなアルゴリズムにしたがってサイトのユーザーを偏った思想に誘導してしまう。それは広告主やアルゴリズムの設計者の意図にも関係なく、かつアルゴリズムの判断基準すら判然としない。しかし、巨大なデータと高速な並列処理によって実現される深層学習や機械学習に基づく機械の判断の正邪を人間個人が判断することは困難であり、人間は機械の判断に盲目的に従ってしまう。Human in the Loop のような牧歌的な対応では、サービスプラットフォームの判断を正常化することはできないため、そこにも機械的な対応が求められる。

人工知能のモデルやアルゴリズムの検定には、バイアスのあるデータセットとバイアスの無いデータセットを準備してその出力を調査することで (a) 判断バイアスのあるシステム、(b) バイアスのデータに弱いシステム、(c) バイアスのデータにも耐性のあるシステムというような三段階の評価フレームワーク⁴⁾をシステムに付随させる。また、データセットのバイアスを低減させる方法として、機械学習のデータセットに対してバイアスを含んだ出力が少なくなるように前処理を行う方法が考えられている。バイアスのあるデータにおいて、バイアスのない出力を増やし、バイアスのある出力を抑制するような関係性を最適化問題として定式化する方法などが考案されている⁵⁾。

クラウドコンピューティングで提供されるサービスにはモバイルネットワークで利用されるものが多い。SNS や EC あるいは情報検索もスマートフォンでの利用が一般的である。今後、自動運転などのサービスが行われるようになると、さらなるネットワークの高速化、大容量化、大規模化が必要になる。移动通信システムは、1980 年代にアナログ方式の第 1 世代が登場した後、1990 年代にはデジタル方式の第 2 世代、世界共通方式である第 3 世代、さらに第 4 世代が導入されるなど、10 年毎に進化し続けている。最大通信速度は 30 年間で約 10,000 倍に高速化した。しかし、2021 年までに、モバイル接続デバイスの数が 116 億台 (M2M モジュールを含む) になると予想される。この数字は、同時期の世界の推計人口 (78 億人) を上回り、世界中のモバイル端末によるデータトラフィック量は 2016 年から 2021 年にかけて 7 倍に増加して、49.0 エクサバイト / 月に達すると予想されている⁶⁾。

そこで、2020 年には、次世代の移动通信システムである「第 5 世代移动通信システム (5G)」

の実現が期待されている。5Gにおいては以下のような性能目標が立てられている⁷⁾。

- ① 拡張モバイルブロードバンド (enhanced Mobile BroadBand)
ピークのデータ帯域 20Gbps、ユーザー体感速度 100Mbps
- ② 大規模マシンタイプ通信 (massive Machine Type Communication)
単位面積接続数が 100 万デバイス / km²
- ③ 超高信頼・低遅延通信 (Ultra Reliable and Low Latency Communication)
無線区間において 1msec の低遅延

新たなモバイルネットワークの出現により、高精細映像と低遅延ネットワークによる遠隔診療や建設機械の遠隔制御、臨場感のあるスポーツ観戦、さらに、自動運転への適用も検討されている。自動車や道路・建造物などの交通インフラに搭載したセンサを活用し、交通状況のリアルタイムな情報収集・解析を行うことによって、高度な運転支援、移動支援を実現すると期待されている。

一方、多様な応用を実現する 5G ネットワークを支えるバックボーンネットワークは、従来の光ネットワークでは限界にきており、より大量のデータを物理的に同じサイズの光ケーブルで配信できるためのマルチコア・マルチモード通信技術やマルチコア・マルチモード一括光スイッチなど超大容量マルチコアネットワークシステムの研究開発が重要である。

(4) 注目動向

生活のなかに深く入り込んできたサービスプラットフォームは、いまや無くてはならないものになった。なかでも GAF A (Google, Apple, Facebook, Amazon) は巨大なプラットフォームを形づくり、今や Google なしで医者も選べないクリニックに行き着くことすらできないという状況もあり得る。Facebook や Instagram で毎日のできごとで友人と心を通わせ、Amazon は小売、物流、エンターテインメント、IT、金融と支配力を拡大し私たちの生活になくしてはならないものになっている。米ニューヨーク大学スターン経営大学院 スコット・ギャロウェイ教授は近著 "The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google" において、過去 20 年の間に四つのテックジャイアンツは歴史上の如何なる存在よりも巨大になり、現代の独占 (Modern Monopolies) を果たしていると述べた⁸⁾。GAF A が基盤としているインターネット事業において彼らは強力なプライベート CDN のバックボーンを利用したタダ乗り事業者 = OTT (Over the Top) と言われてきたが、いまや消費者の支持を得たコンテンツには逆らうことができない。

金盾 (Great Firewall) によって GAF A の侵攻を食い止めた中国では、Baidu や Alibaba のような GAF A に代わるプラットフォームが育っている。国内では利用者がより深いパーソナル情報をアップロードするサービスの共創⁹⁾ が起こり、新しいペイメントサービスや芝麻信用のような個人の信用レイティングが社会生活を円滑にしている。こうした社会形成はプライバシーという観点でビッグブラザーであると思われがちだが、サービスプラットフォームの視点から見ると「より良い生活を得るために情報を提供し、適切なサービスを受け取る」という行為であり、西側諸国で Google や Amazon を利用している利用者心理と変わらない。

インターネット黎明期にあったオープンで公平なピアツーピアネットワークの文化は、現代

の強力なサービスプラットフォームによってインターネット上のデータが独占されたため、一極集中した構造になっている。古きインターネットはノード間の情報接続を実現するハイパーリンクと、情報のリッチな表現をはたす HTML、その世界を覗く WEB ブラウザーによって互いに平等なピアツーピアのネットワークを構成してきた。しかし現代の Google は検索のクローリングを続けながら、WEB サーバー間のリンクの繋がり、HTML によって表現された情報の意味、セマンティックグラフを Knowledge Graph に集約し、WEB 検索の枠を超えインターネットに存在している情報のセマンティックを集中管理している。また、WEB ブラウザーに仕込まれたトラッキングスニペットはブラウザー上のアクションや GPS などのユーザーのコンテキスト、行動データを集約してパーソナルプロフィールデータを集約している。こうして、情報のゲートキーパーの役割を果たしながら広告媒体の莫大な利益を吸い上げている。Google や Amazon のようなインターネットの巨大なサービスプラットフォームは、インターネット全体を支配する巨大帝国となっている。

サービスプラットフォームの大量のデータとユーザー情報は経済活動の極めて高い効率化をもたらす生産性を向上させる。そこでは、データの価値が生まれる規模（十分な相関や特徴量のとれる量）、クリティカルマスに達するオーディエンス・コミュニティを構築することでネットワーク外部化する価値を生み出す¹⁰⁾。プラットフォーマーはオーディエンスのスイッチングコストを高めつつ、そこで取引されるトランザクションのフリクションを減らしていくことでビジネスを効率化する。デジタル情報を扱う情報商品の流通コストはゼロに近くても情報の開発コストはゼロではない。サービスプラットフォームは参加者をサービス提供者にすることでその情報の開発コストもゼロにする。YouTube はプロシューマーが映像を作り、Uber は運転者をリソースとする調達のオンデマンド化をもたらす。WeChatPay はユーザーが預けたキャッシュフローを活用した運用によって、より複雑なマネタイズを実現している。サービスプラットフォームのビジネスモデルでは、限界費用は常にゼロに近づいている。

現代のフリーミアムプラットフォームのアドテクビジネスが経済に与える影響を過小評価してはいけない。プラットフォーマーが吸い込んでいるのは現実社会の広告宣伝費だけではなく、EC への転換など商流の相当部分を占める販売管理費全体である。経済活動の全てを効率化し、冗長なプロセスをバイパスすることで、企業は営業部門も物流部門もデータだけに依存する最適化されたものになり、物理的な営業所も営業社員も存在しなくなる。

サービスプラットフォームによる生産性の増大は正帰還であるため、富は偏在し、限界費用はゼロに近づいていく¹¹⁾。デジタル世界の資源は無限に思えるようなデータであるため独占がいままで見たことのないレベルに達することが予想できる。GAFA の富の独占が行き過ぎて資本主義すら壊れてしまうのではないかということをおそらく GAFA 自体もコントロールできないと思われる。

Amazon は書籍の通信販売から始まったが、いまや日用品から衣料品、食品にまで商材を拡大し、さらに実店舗でのビジネスまで行っている。さらにそのバックエンドとしての流通においても非常に大きなビジネス展開をしている。自身のコンピューティングパワーを用いて、世界でも最大級のクラウドサービスも実現している。一方の Google もパソコンにおける検索サービスと広告ビジネスから端を発したが、いまや携帯電話のプラットフォームである Android を押さえ、自動運転やロボットの開発にも乗り出している。両者は音声プラットフォームで激しい争いを繰り広げており、それは他の産業セクターも巻き込んでいる。これらの背景にはデ

一タの独占という状況があり、誰もその制御が行えないという問題がある。

ヨーロッパにおいては GDPR（General Data Protection Rule）を発効し、彼らの独走を止めようとしている。我が国においても、独占禁止法による規制の導入が検討されている。

（5）科学技術的課題

人工知能に関しては、詳細は他の区分に譲るが、プラットフォームとして社会のインフラになるためには、公正・公平・透明性の確保が重要である。そのためにも説明可能な人工知能や、人工知能プログラムの品質保証なども重要な課題である。

5Gにおいては、無線通信技術の研究開発はもちろん必須であるが、ネットワーク構築・運用技術もともに研究開発をするべきである。さらに、エッジコンピューティングの効果的な利用方法や、さまざまなビジネスのプラットフォームとして利用されるためのビジネス開発の研究開発も必要であろう。

（6）その他の課題

新たなサービスの創出のためには、既存の規制の緩和と新たな規制導入の検討や促進策、価値の再配分の透明性、公平性を担保する事が必要となる。また、既に標準化やプラットフォーム構築が進められている動きとの連携が求められる。

規制緩和と新たな規制の必要性

既存規制により新たなサービスの創出が阻まれるという損失や、サービスプラットフォームによるなし崩しの規制緩和が生じないように、適切な規制緩和が求められる。

一方、GAFA に対する GDPR のように、サービスプラットフォームが寡占化し、暴走することがないように、新規制の導入も検討しなければならない。サービスプラットフォームはすでにグローバル化しており、徴税やプライバシー保護、商習慣などにおいて国際的な連携・協調が必要である。

価値の再配分の透明性、公平性を担保するしくみ

サービスプラットフォームでは、資産のシェアだけでなくユーザー間の信頼や、ユーザーエクスペリエンスを取り扱う複雑なシェアリングエコノミーを提供する。この維持発展には、参画するステークホルダー間において、価値の再配分の透明性、公平性を担保する仕組みが重要となる。ここではブロックチェーン技術の利活用が期待されるが、規制とのバランスが重要になってくる。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	↘	<ul style="list-style-type: none"> データ解析の基礎的技術、大量データの処理技術などは継続的に進んでいる。しかしディープラーニング等に利用される国産 GPU や FPGA はなく、専用チップの開発も進まない。 プラットフォーム独占や中立性の基礎的研究が欠けている。 個人情報の扱いに関する先行研究もない。
	応用研究・開発	△	↘	<ul style="list-style-type: none"> プラットフォームのデータ解析に展開する実装は進んでいない。 新しいデータ活用、独自技術なども進まない。プライバシー議論が先行し、データ活用が進まない。 人工知能開発を闇雲に規制する議論があり、人材が散逸している。 5G URLLC/mMTC は先送りされている。 人工知能のエッジコンピューター化はすすんでいない。 ブロックチェーン実装は投機的な仮想通貨に偏っている。 ペイメントサービスは黎明期にあり、シェアは依然として些少である。 国民 ID（マイナンバー）も利用の広がりを見せていない。
米国	基礎研究	◎	→	<ul style="list-style-type: none"> シリコンバレーを中心に依然としてソフトウェアの主導権を握っている。オープンソースの開発も技術をリードしている。 データの活用や人工知能、自動運転などの先端研究も先行している。
	応用研究・開発	◎	→	<ul style="list-style-type: none"> GE が Predix で産業界のサービスプラットフォームに挑戦したが他要因で躓いている。 GAF A の独占は強く、Uber AirBnB と続いている。Netflix、Amazon、Apple の放送通信の OTT(Over the Top) 事業参入が盛んでコンシューマータッチポイントを独占しようとしている。ケーブルテレビの契約をやめる動き（コードカット）も多くなっている。 クレジットカードと Paypal を押しのけた新しいペイメントは生まれにくい。 5G に対する動きは弱い。
欧州	基礎研究	◎	→	<ul style="list-style-type: none"> 基礎的なソフトウェア技術は米国依存。自動運転技術の開発は活発である。 5G の URLLC/mMTC に積極的。情報のオーナーシップに関わる議論を GDPR で実装、プラットフォーム規制の基礎的機能を研究。
	応用研究・開発	○	→	<ul style="list-style-type: none"> GAF A に対する独占、プライバシー規制を先行させ、制裁金による徴税機能を果たしている。 一部の電子政府で国民 ID システムによる行政システムの開放などの先行事例がある。 ブロックチェーンを用いた貿易データ管理などスマートコントラクトの実装例もある。
中国	基礎研究	◎	↗	<ul style="list-style-type: none"> データ処理や人工知能研究、自動運転技術などの研究も進み、シリコンバレーに追いつく勢いである。 5G については機材メーカーを中心に積極的にミリ波利用などで先行し、URLLC/mMTC に対しても積極的な実装を進めようとしている。
	応用研究・開発	◎	↗	<ul style="list-style-type: none"> GAF A の侵入を阻む金盾の内部でサービスプラットフォームの構築が進んでいる。 個人データの共創が進み、プライバシーに関する異なる価値観を創出している。 ペイメントサービスは先行して普及しており、世の中の動きは早い。 ブロックチェーンはビットコインのマイニングが中心でスマートコントラクトなどは目立たない。

（8）参考文献

- 1) 安宅和人 2017 「経済産業省産業構造審議会新産業構造部会 February 13, 2017」 シン・ニホン” Ai x データ時代における日本の再生と人材育成」 http://www.meti.go.jp/committee/sankoushin/shin_sangyoukouzou/pdf/013_06_00.pdf
- 2) アレックス・モザド（著）、ニコラス・L・ジョンソン（著）、藤原朝子（翻訳） 2018 『プラットフォーム革命——経済を支配するビジネスモデルはどう機能し、どう作られるのか』 英治出版
- 3) 山下克司 2017 『“3.2.3 モノ・ヒト・コトのスマートなサービス化技術 P166-186』 研究開発の俯瞰報告書 システム・情報科学技術分野（2017年）CRDS 科学技術振興機構
- 4) Biplav Srivastava and Francesca Rossi, “Towards Composable Bias Rating of AI

- Services,”
AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society http://www.aies-conference.com/wp-content/papers/main/AIES_2018_paper_65.pdf
- 5) F.P. Calmon*1, D. Wei, B. Vinamuri, K. N. Ramamurthy, and K. R. Varshney, “Optimized Pre-Processing for Discrimination Prevention,” 31st Annual Conference on Neural Information Processing System <http://papers.nips.cc/paper/6988-optimized-pre-processing-for-discrimination-prevention.pdf>
 - 6) Cisco Visual Networking Index、https://www.cisco.com/c/ja_jp/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html
 - 7) 「第5世代移動通信システム（5G）の技術的条件」、新世代モバイル通信システム委員会 http://www.soumu.go.jp/main_content/000556416.pdf
 - 8) Scott Galloway 2017 “The Four: The Hidden DNA of Amazon, Apple, Facebook and Google” Bantam Press (2017/10/5)
 - 9) Spohrer, J., Anderson, L., Pass, N., and Ager, T. (2008) “Service science and service-dominant logic,” Otago Forum 2: Academic Papers. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.486.3642&rep=rep1&type=pdf>
 - 10) アルスタイン・マーシャル W., パーカー・ジェフリー G., チョーダリー・サンギート・ポール, 有賀裕子 (訳) (2016) 「パイプライン型事業から脱却せよ プラットフォーム革命」『Harvard Business Review 2016年10月号』 p27-38 ダイヤモンド社
 - 11) 丸山俊一, NHK 「欲望の資本主義」制作班, “欲望の資本主義” 東洋経済新聞社, 2017

2.4.6 IoT アーキテクチャ

(1) 研究開発領域の定義

膨大な数のセンサーや端末がネットワークに接続される IoT 時代において、実世界とサイバー世界を高度に融合するコンピューティング環境を実現するための技術である。

実世界を構成するモノ・ヒト・コトの状況を認識するセンサー技術、それらに作用や情報を与えるアクチュエーション技術、デバイスそのものの構成法、認識処理方式、作用や表示方式等の情報通信技術をはじめとして、長期稼動を実現するための電力供給技術、必要に応じて機器や端末が自律的に移動する技術、ビッグデータ分析を可能にする機械学習 / AI 技術が含まれている。

ここでは、実世界との境界 (エッジ) にあつて Society 5.0 を実現する情報流の源でありかつ作用点としての観点から関連する技術、動向と課題を俯瞰する。

(2) キーワード

エッジコンピューティング、フォグコンピューティング、クラウドコンピューティング、モバイルエッジコンピューティング、5G、ストリームコンピューティング、Internet of Things、スマートセンサ、エネルギーハーベスト、VR、ウェアラブル、パーソナルデータ / 個人情報の保護 / 活用、アクチュエーション

(3) 研究開発領域の概要

[本領域の意義]

膨大な数のモノがネットワークに接続されるようになると¹⁾、現在のクラウドコンピューティングはネットワークに起因する遅延、様々なデバイスへの対応、地域性・局所性への対応などの観点で必ずしも最適な解とはならなくなる。モノがクラウドに接続される形態に加えて、エッジ側に機能追加することも必要となる。

例えば、スマートグリッドにおける高速デマンドレスポンス²⁾では、数秒オーダーの速度で需要側に設置されたスマートメータと需給調整を行うことが必要となる。膨大な数のスマートメータからデータを収集して、需給調整方法を計算し、需給側に対して制御を行うことを考えると、集中管理のクラウドでは遅延の制約を満たすことが難しくなる。エッジ側とクラウド側とが連携しながら処理を行う仕組みが必要となる。

実世界と接し、そこから様々な状況を認識し情報を取得するセンシング、実世界に作用を与えるアクチュエーションといった技術、実世界に接するエッジでのスマートコンピューティング技術、エッジで得られた情報が構成するビッグデータを大量の計算機資源で制御するクラウド技術と分析する AI に代表される認識技術、そしてエッジとクラウドをつなげる様々な情報通信技術が本領域には含まれる。IoT アーキテクチャは、これらの広範な技術を統合した上に成り立ち、実世界と情報空間の間に位置し、利用者にとって最も身近に感じられる重要な位置づけにある。

[研究開発の動向]

コンピューティング分野は、時代とともに何度もパラダイムシフトを繰り返してきた。1960年代にはユーティリティコンピューティングという概念が生まれ³⁾、その後、クラスターコンピューティング、さらに1990年代に入ると、ユビキタスコンピューティングの考え方が登場し、ヒューマンセントリックでコンテキストウェアなサービスが創出された。また、インターネット上の多くの計算資源を結びつけ、ひとつの複合したコンピュータシステムとしてサービスを提供するグリッドコンピューティングも登場した。2000年代に入ってから、大規模データセンターを背景としたクラウドコンピューティングが世界を席卷した。2000年代後半からモバイルクラウドコンピューティングが唱えられはじめ、今のフォグ/エッジコンピューティングへと発展している。

これらの変遷の背景には、エンドユーザの要求とハードウェアの進化がある。フォグ/エッジコンピューティングが登場した背景も、エンドユーザの要求の変化とデバイスの高性能化にある。クラウドコンピューティングでは通信遅延が大きく、モビリティサポートへの対応が不十分、大きな通信オーバーヘッド、コンテキストウェアネス対応が困難などといった課題を抱えていた。

通信技術

5Gの登場が現実味を帯びてきていることもあり、産業界においてもフォグ/エッジコンピューティング分野での動きが活発になりつつある。5Gの持つ「低遅延」、「大容量」という特徴を生かして、アプリケーションの応答性の改善や、ユーザエクスペリエンスの向上などが期待されている。OpenFog Consortium⁴⁾、OpenCORD initiative⁵⁾、ETSI Mobile Edge Computing(MEC)⁶⁾、Field System⁷⁾、Edge Cross⁸⁾などのコンソーシアムも設立され、それぞれが主導権を獲得すべく活動をしている。

BLE (Bluetooth Low Energy) や 920MHz 帯を活用する Wi-SAN などの近距離省電力で小規模端末間通信を対象とするもの、さらに LPWA (Low Power Wide Area) と呼ばれるノイズレベルのサブ GHz 帯の無線信号を低ビットレート、超低消費電力でサポートする広域無線網も注目されている⁹⁾。

センシング技術

既存のセンシング機器は MEMS (Micro Electro Mechanical Systems) 技術を用いた小型化、省電力化、さらにスマート化が推進されている。メインプロセッサが休眠できるアーキテクチャの採用によって省電力化が進められ、携帯端末上でのこれらの個々のセンシング機能や通信機能のオンオフを気にする必要が低下している。

近年のスマートフォンでは ARM の big.LITTLE アーキテクチャと呼ばれる高性能コアと低性能コアを同一ダイ上に混載して、常時センシングを止めずにかつ省電力性能を上げる方式が一般化し、ARM はそれを更に DynamicIQ 技術¹⁰⁾ に発展させた。Apple のモーションコプロセッサは低性能で省電力コアをセンサーハブとしてメインプロセッサ外に独立させた方式で、センサデータの一次処理を担うなどの役割ももつ。

今後注目すべきはセンサーのスマート化である。センサーにより獲得された生のデータ量は目的とする情報にまで認識・分析されれば大幅に圧縮することができる。また、認識された情

報をクラウドに上げることなくその場で活用できる機会も増える。データ量の軽減のみでなく、カメラ映像からヒトのみを抽出し、映像的に匿名化処理を施す、人流状況の統計的処理をその場で実施するなどプライバシーに配慮した試みも実用化段階にきている¹¹⁾。

機械学習技術

携帯端末での機械学習機能では、iOSのCoreMLやGoogleのTensorFlowとその携帯端末版であるTensorFlow Liteを内蔵するML Kitは、整備されてきたハードウェアをサポートし現実的な文字や画像などの認識機能を備えつつある。いずれも機械学習の処理としては認識フェーズをサポートしているが、学習フェーズはより大量の計算機リソースを必要とするためにクラウドベースの対応となっている。GoogleではこのためにML KitをmBaaS（mobile Backend as a Service）であるFirebaseの一部として実装している。さらにML KitはAndroid/iOSともにサポートしており、今後の爆発的な普及が予想される¹²⁾。

アクチュエーション技術

実世界に影響を与える作用を実現するものであり、携帯端末での情報の提示、街中でのデジタルサインエージ、機械可読マーカ、タッチデバイスに導入されたAppleのTaptic Engineなどの力覚生成機器はウェアラブル機器のインタフェースとしても多用されるようになってきており、今後は広範囲に力覚を用いたUIが適用されていくと思われる。没入型のVR機器を用いた入出力一体型インタフェースもOculus Goなどのように小型化しスマートフォンを必要としないものが出荷されており、既に普及期に入り始めたといえる。

電力供給技術

IoTのエッジでの小型端末に必須の要素である電力供給をいかに実装するかは常に課題である。大容量二次電池であるリチウムイオン電池、加工成形に利するリチウムポリマー電池は成熟期にあり、全固体電池技術によるさらなる高性能化が期待され燃料電池車をとばして一気に電気自動車への移行が急激に加速した¹³⁾。今後は電気二重層コンデンサ（Electric double-layer capacitor、EDLC）やリチウムイオンキャパシターなどの高効率キャパシターの実用化のための開発、IoT機器に特化したエネルギーハーベスターの開発に注目が集まっている。環境発電技術では光発電以外に、レクテナによる電磁波や近距離での無線給電技術、音や振動による発電の研究も実用間近である。

ウェアラブル技術

ウェアラブル端末は新たな素材を開発することによって衣服や靴をインテリジェント化する医療系、フィットネス系の試みが注目されている¹⁴⁾。課題は電力供給、部品清掃、製品寿命のアンバランスなどがあげられる。

（４）注目動向

【新展開・技術トピックス】

フォグ／エッジコンピューティング分野の特徴は、プレイヤーの多様化である。もともとは、シスコがフォグコンピューティングを2012年に提唱¹⁵⁾したように、IT企業がフォグ／エ

ジコンピューティングを主導してきた。これに対して、昨今は、通信事業者や製造業などからフォグ/エッジコンピューティングに参入するプレイヤーが増えてきている。通信事業者からは Mobile Edge Computing(MEC)、製造業からは GE の Industrial Internet Consortium¹⁶⁾、ファナックの Field System⁷⁾、三菱電機の Edge Cross⁸⁾ などである。

このような流れの中で求められるものは、多種多様なアプリケーションの要件を理解することに加えて、これらの要件を抽象化してフォグ/エッジコンピューティングの設計につなげていくことである。現在は、個別のアプリケーションに特化したフォグ/エッジコンピューティングにとどまっている。特化型フォグ/エッジコンピューティングの開発を通して要件を一つ一つ積み重ねていきながら、抽象化につなげ、汎用的なフォグ/エッジコンピューティング基盤の構築につなげていかなければいけない。

また、IoT データを単一システム内、あるいは、複数のシステム間をまたいで流通させるためのメタデータの記述や流通プロトコルが重要である。インターネットが TCP/IP によって発展したように IoT システムのさらなる発展には、汎用的な流通プロトコル (MQTT, CoAP, HTTP REST, SOX, SPAQL) の確立が重要な課題である。

センシングの注目動向としては深度センサーの利用の多様化である。自動運転用の LiDAR に端を発し、商用ベースでは Kinect、Google の Project Tango、Apple の FaceID など、ますます小型化と用途の多様化が目立っている。今後は多眼のカメラレンズ搭載機器がこのような立体空間認識機能を備えていくはずである。

モビリティの大きな動向としては、無人タクシーや物流の先導追従運転など自動運転の社会への導入が始まり、ポスト自動運転の世界を考えた動きが始まっていることであろう。トヨタの e-Palette を始めとするモビリティをプラットフォーム化する動き¹⁷⁾は MaaS(Mobility as a Service) を実現しようとする交通業界全体からさまざまな提案がでてくるものと思われる。

個人情報データは保護すべき対象とされるが、それを安心して活用できる基盤として情報銀行という仕組みが立ち上がりつつある。個人がその健康情報データや購買データを信託し、それを非識別化加工を実施した上で、活用するサービス企業とやりとりし、銀行のように一部の利息が個人情報提供者に戻ってくる仕組みである。情報銀行はこれらの個人情報を中央集権的に管理する仕組みであるが、一方では PLR (Personal Life Repository) にもとづいた個人の医療・介護記録を自身で管理し、流通の制御を個人にゆだねる分散 PDS (Decentralized Personal Data Store) の仕組みの実証も始まっている¹⁸⁾。高齢化が進む社会でのパーソナルデータ活用の推進の意味でも注目すべき試みである。

自動車保険の分野でもセンシングを活用し、あらたなサービスが開発されている。あいおいニッセイ同和損害保険は、トヨタ自動車のテレマティクスサービス「T-Connect」のナビから、スマートフォン等を通じて取得した車両運行情報を、走行距離に基づいた保険料の算出や安全運転アドバイスなどのサービスに活用している¹⁹⁾。

[注目すべき国内外のプロジェクト]

いまや携帯電話/スマートフォンは情報インフラの一つであり、どのようなユーザがどこで何をしているかというコトの情報化には欠かせない仕組みである。加古川市は町の見守りサービスの基盤を「かこがわアプリ」と 900 機の見守りカメラ、公用車および日本郵政の配達者に装備した V2X 機器で実現し、子供や高齢者が携帯する BLE タグ位置を検出できるサービス

を実施している²⁰⁾。ここで注目すべきはこれら見守りサービスを実施する民間3社で互いの見守り網となる機器の利用を相乗りさせることに成功していることである。このようなアライアンスは今後も拡大していくことが期待できる。

最新のセンシング技術として注目される深度センサー利用は Google の Project Tango で深度センサーが用いられた端末が普及する兆しがあったが、光学カメラベースに技術を移転し VR/AR 技術の携帯端末での利用・普及が始まっている。特殊な端末から、光学カメラというほとんどの携帯端末が有するセンサーに軸足を変更したことによって、VR/AR 技術は数億の端末によって利用可能な技術に生まれ変わりつつある。特に高級なスマートフォンにおいては、光学センサーとして複眼のレンズを搭載しており、既に簡易に高度かつ精細で、焦点や光量の破綻のない写真撮影が可能になっている。これが空間認識に利用され、VR/AR 技術が Project Tango レベルの点群データを活用できるようになるのも遠くないと考えられる。

Google の Tensor Processing Unit に端を発する機械学習専用プロセッサも近年では携帯端末に搭載されるレベルになってきている。中国の麒麟、Apple の A12bionic などは、プロセッサダイの半分近くをニューラルネットワーク処理用の専用プロセッサが占めている。これまでは GPU を用いていた AI 処理計算に対して、より効率が良く演算器数の多い専用プロセッサが追加されていくと思われる。すでに製造工程におけるダークシリコン問題や多大な生産コスト増などで汎用プロセッサの純粋な意味でのムーアの法則は崩壊している。いよいよポストムーアの法則時代の個性的なプロセッサ開発や新しいアーキテクチャを探求していく試みが始まっているといえる²¹⁾。

[コンソーシアム]

以下のような様々なコンソーシアムが立ち上がり、業界を横断して連携・競争が激しくなっている。

IoT 推進コンソーシアム²²⁾

総務省と経産省が中心となり、産学官が参画・連携し、① IoT に関する技術の開発・実証及び標準化等の推進、② IoT に関する各種プロジェクトの創出及び当該プロジェクトの実施に必要なとなる規制改革等の提言等を推進している。設立当初は 700 社が参加していたが、2018 年現在で 3,600 社が参加している。

スマート IoT 推進フォーラム²³⁾

上記「IoT 推進コンソーシアム」の下に、IoT 関係の技術開発・実証を推進する技術開発ワーキング・グループとして設置された。IoT・BD・AI 等に関する技術の開発・実証の推進、IoT・BD・AI 等に関する技術の標準化や国際展開等を推進している。

oneM2M²⁴⁾

さまざまなハードウェアやソフトウェアに容易に埋め込むことができ、現場の無数のデバイスを世界中の M2M アプリケーションサーバーに接続することができる、共通の M2M サービス層に必要な技術仕様を開発することを目標に、TTC など世界の主要な標準化団体が設立した団体である。

AllSeen Alliance

Qualcom が開発した通信規格を中心として、IoT 機器の相互接続を実現することを目的として、2013 年に設立された。その後、もう一つの IoT フレームワーク推進団体である Open Connectivity Foundation²⁵⁾ と協力して一つの IoT 標準としてオープンソースプロジェクト IoTivity を推進している。

OpenFog Consortium⁴⁾

効率的かつ信頼性のあるネットワークとスマートな端末のためのフレームワークの構築を目指し、ネットワーク遅延、移動端末への対応、通信帯域障壁問題、システムとクライアントの分散調整などの技術課題に取り組んでいる。ARM, Cisco, Dell, Intel, Microsoft, プリンストン大学が 2015 年に設立したコンソーシアム。

Central Office Re-architected as a Datacenter⁵⁾

マイクロデータセンターの構築を目指したコンソーシアム。AT&T, SK Tlecom, Verizon, China Unicom, NTT コミュニケーションなどが参画。

ETSI MobÖe Edge Computing(MEC)⁶⁾

無線アクセスネットワーク (RAN) にエッジコンピューティング機能配備を目指して、エッジサーバについての技術要件とアーキテクチャの議論を行っている。通信キャリアや装置開発ベンダ、OTT などが参加している。

FIELD System⁷⁾

ファナックが開発する製造業向けエッジコンピューティングプラットフォーム。Cisco, Rockwell Automation, Preferred Networks, NTT, NVIDIA, 日立製作所などが参画。

Edge Cross⁸⁾

FA 向けエッジコンピューティング。アドバンテック、オムロン、NEC、日本 IBM、日本オラクルが参加し、三菱電機が幹事会社となっている。

Automotive Edge Computing Consortium²⁶⁾

自動車向けエッジコンピューティング。Intel, Ericsson, デンソー、トヨタ自動車、トヨタ IT 開発センター、NTT、NTT ドコモなどが参加している。

Edge Computing Consortium²⁷⁾

OT と IT の協調を目指すエッジコンピューティング。Huawei, Shenyang Institute of Automation of Chinese Academy of Sciences, China Academy of Information and Communications Technology, Intel, ARM, iSoftStone が参画している。

(5) 科学技術的課題

フォグ/エッジコンピューティング分野での研究開発領域は、大きく「クラウドフォグ/エッジ連携機構」「フォグ/エッジデバイスの仮想化」「フォグ/エッジでのアプリケーション開発環境」「フォグ/エッジデバイス、ネットワークでの資源管理」「ストリームコンピューティング」「セキュリティとプライバシー」とに分けることができる。

クラウドフォグ/エッジ連携機構

第一の課題は、フォグ/エッジノードとクラウドノードとの間でタスクやサービスをどのように分割するかにある。タスク分割、タスク割当問題は、分散システムや並列コンピューティングなどの分野では多くの研究がなされてきたが、フォグ/エッジ環境でのフレームワークは残念ながら未だ存在しない。資源リッチなクラウドから、資源制約のあるフォグ/エッジに、性能やプライバシーを考慮しながらタスクを効率的にオフロードするのは大きなチャレンジである。

第二の課題は、フォグ/エッジコンピューティングでのサービス指向コンピューティングの難しさにある。フォグ/エッジコンピューティングは、センサー、アクチュエータ、エッジデバイス、クラウドサーバそれぞれが多様であり、それらが分散しているとともに、アプリケーションも多種多様であるため、サービスのセマンティクスのあり方が問題になる。

第三の課題は、ドメイン間連携にある。フォグ/エッジコンピューティングは、単一の事業者がクラウドからフォグ/エッジまで統合してサービス提供するとは限らない。そのため、エンドツーエンドでサービス提供を行うためには、ドメイン間での連携が必須となる。多種多様な要件を満たすことのできるドメイン間連携機構は大きなチャレンジである。

フォグ/エッジデバイスの仮想化

第一の課題は、フォグ/エッジデバイス向けのVM(Virtual Machine)やコンテナ技術である。フォグ/エッジデバイスは資源制約の中で動作させなければいけないため、従来のハイパーバイザやコンテナ管理ソフトが使えらるとは限らない。フォグ/エッジ向けのハイパーバイザ、コンテナ管理ソフトの開発が必要である。

第二の課題は、VMやコンテナのマイグレーションである。フェールセーフでフォールトトレラントなシステムを実現するためには、マイグレーションが必須である。IoTデバイスの移動にあたってサービスマイグレーションが必要となる。すでにクラウド環境においては、ライブマイグレーションが実現されているが、同様のことが資源的な制約のあるフォグ/エッジでも行えるような環境が必要になる。

第三の課題は、マイクロサービスを実行するコンテナの配置にある。制約のある資源環境下において、所望のサービス要件を満たすためのコンテナの最適配置は重要な課題である。

フォグ/エッジでのアプリケーション開発環境

ドメイン特化型のアプリケーション開発環境は既に存在するものの、汎用型のアプリケーション開発環境は存在しない。ソフトウェア定義やソフトウェア制御技術を使うことで、汎用型の開発環境を実現できる可能性がある。アプリケーションからサービスとサービス依存グラフを抽出し、サービスをフォグ/エッジデバイスに展開するミドルウェアの開発が必要である。

フォグ/エッジデバイス、ネットワークでの資源管理

フォグ/エッジデバイスは資源制約があるため、CPU、メモリ、ネットワーク、センサー、アクチュエータなどの資源を適切に分配しなければいけない。このためには、フォグ/エッジデバイスの資源を効率よく推定する機構、公平にかつ所望の QoS(Quality of Service) を満たすように資源を割り当てる機構、SDN(Software Defined Network) を用いてネットワーク資源を適切に割り当てる機構などの開発が必須である。

ストリームコンピューティング

多種多様な IoT デバイスから収集した膨大な異種データから、重要な特徴を抽出するオンラインデータ分析プラットフォームの開発はこれからの課題である。ストリーム処理、分散機械学習、オンライン機械学習などとともに、動的時間伸縮法 (DTW: Dynamic Time Warping) などのパターンマッチング技術を用いたストリームデータからの特徴抽出なども含めて、幅広い研究開発が必要である。

セキュリティとプライバシー

フォグ/エッジデバイスは、エンドユーザに近く、クラウドと比較してセキュリティリスクの不安がある。また、資源制約もあるため、DoS(Denial of Service) 攻撃などのセキュリティ攻撃にも弱い。さらに、エンドユーザに近いことから、プライバシーに対する考慮も必須である。セキュリティとプライバシーはアプリケーションごとに要件が異なるため、アプリケーションごとに、一つ一つ地道に考えていくしかない。

(6) その他の課題

フォグ/エッジコンピューティングを設計するためには、現場に入り込んで顧客のニーズを把握することが大切である。机上で議論するだけでは、現場に適用できないシステムとなってしまう。スマートシティにしてもスマート工場にしてもスマートグリッドにしても、顧客の価値を明らかにしながら設計していかなければいけない。

そのためには、研究者と現場とをつなぐ触媒役となりえるカタリスト人材が必要である。技術開発を行う人と現場とを上手につなぐ役割である。このような人材が圧倒的にわが国には少ないことが、「技術で勝ってビジネスで負ける」一因である。

わが国の研究開発予算の用途は、技術開発に重点的に振り向けられている。これに対して欧米の研究開発予算は、カタリスト人材などを含む技術開発以外にも振り向けられていることを踏まえ、技術開発以外のリソースに予算配分をしていくことが重要である。

これは標準化でも同様である。フォグ/エッジコンピューティングを展開していくためには、標準化議論も避けて通ることができない。技術的な観点からのみ標準化作業に携われる人だけでは仲間を作って事業につながる標準化に結び付けることが難しい。事業戦略を考えながら仲間作りを行うだけでも多大なリソースを必要とすることから、このような人材にも予算配分をしていくことが重要である。

アーキテクチャ設計は技術開発項目に含まれることになるが、学術的成果として認められづらいこともあり、なかなかアーキテクチャ議論にリソースを割くことができない状況になっている。そのため、研究開発プロジェクトにおいては、意識的にアーキテクチャ議論を推進する

仕組みがあることが望ましい。抽象化して議論する場を提供することが、わが国のアーキテクチャ人材の育成にもつながる。

プライバシーや個人情報の保護の観点からは、保護する対象がこれまでのように申込書等に記入し、個人が提供を意識しているもの以外に、センシングを通じて無意識のうちに生産、収集される多種多様なデータも対象になる。個人はデータの活用について深い理解をしないうちに、規約に同意することが考えられる。そこで、情報の利用についてサービス開始時にパーミッションを得るだけでなく、サービス利用中においても利用者からの問い合わせに対して適正な説明が可能な仕組みづくりが求められるだろう。

自動化された処理はローンの審査や人事・採用評価などに及びつつあり、その究極的な様相を見せているのが中国 Alibaba の Alipay で与信システムとして利用されている Sesame Credit Score(芝麻信用)である。ユーザのあらゆるネット活動と個人特定のできる大量の監視カメラによるユーザの評価を 950 点満点で実施し人物評価がなされ、その数字のみが一人歩きしている。このスコアはいまや中国社会全体の治安にも影響するほどの効力があり、一旦低い評価を受けるとそこから抜けだせないバーチャルスラムと呼ばれる新たな貧困層を生んでいるともいわれている。その一方では 2018 年 5 月から EU で発行された GDPR(EU 一般データ保護規則)はこのような AI による自動化された評価や審査を禁止する方向にある。この両者の動きは両極にあるともいえ、日本、米国も GDPR 的な規制がないままであると今後は経済的にも社会的にも大きな問題が発生しかねない。

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	△	→	・アプリケーション/サービスにまで踏み込んだ基礎研究は少ない。アーキテクチャ議論にも弱い。 ・文科省/JSTのAI/IoTを推進するサポートがあるも、他国の競争についていけていない。
	応用研究・開発	○	↗	・製造業を中心に、実用化が確実に進みつつある。 ・個人情報保護法の改正、官民データ活用推進基本法の制定などでデータ活用の推進が期待される。
米国	基礎研究	◎	→	・アプリケーション/サービスにまで踏み込んだ基礎研究を幅広く進めている。 ・Google やスタートアップ等、革新的なセンサー技術や AI 技術の本格応用の研究開発が順調。
	応用研究・開発	◎	→	・産業界コンソーシアムを中心に、動きが活発である。 ・自動運転の実用化や、GE の Industrial Internet の進行、Qualcomm の AllSeen Alliance、Uber/AirBnB などの新規サービスの隆盛などどまるところを知らない。
欧州	基礎研究	○	→	・EU が継続的に支援しており、アーキテクチャ議論などにも強い。
	応用研究・開発	◎	↗	・ドイツ企業を中心として盛んな研究開発を進めている。コンソーシアムの作り方、場の作り方がうまい。 ・Smart City を標榜するスペインの各市プロジェクトがあるも、GDPR 発行後の個人情報保護の重視政策による圧迫に注目。
中国	基礎研究	△	→	・日本と同じレベルにある。アーキテクチャ議論にも弱い。ただし、独自のアーキテクチャや他国に依存しないサービス実現の必要性から、麒麟などのシリコンチップおよび端末製造技術の進展が著しい。
	応用研究・開発	◎	↗	・Huawei などのメーカーと Alibaba などサービス事業者が活発な動き。 ・個人情報配慮が軽く、急速に社会が変化している。
韓国	基礎研究	○	→	・Samsung と LG を中心にディスプレイ技術とモバイル/ウェアラブル端末部材を中心に技術開発が活発。
	応用研究・開発	○	↗	・スマホ決済サービスの進展と定着、Hyundai 等自動車メーカーの実証実験。 ・個人情報保護が緩和されビッグデータ活用が急速に拡大中。

(8) 参考文献

- 1) 総務省、「IoT デバイス 1 の急速な普及」、情報通信白書平成 30 年版
- 2) 経済産業省、「ダイヤモンドリスポンスについて」、第 4 回 総合資源エネルギー調査会 電力・ガス事業分科会 電力・ガス基本政策小委員会 制度検討作業部会、2017 年 4 月 20 日 http://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/seido_kento/pdf/004_s01_00.pdf
- 3) Simson Garfinkel, "The Cloud Imperative", MIT Technology Review, October 3, 2011 <https://www.technologyreview.com/s/425623/the-cloud-imperative/>
- 4) <https://www.openfogconsortium.org/>
- 5) <https://opencord.org/>
- 6) <https://www.etsi.org/technologies-clusters/technologies/multi-access-edge-computing>
- 7) <https://www.fanuc.co.jp/ja/product/field/index.html>
- 8) <https://www.edgecross.org/ja/>
- 9) 成長期を迎えた LPWA の将来と課題 <http://jbpres.ismedia.jp/articles/-/52839>
- 10) ARM が bit.LITTLE アーキテクチャを AI 拡張した技術 DynamicIQ <https://community.arm.com/processors/b/blog/posts/arm-dynamiq-expanding-the-possibilities-for-artificial-intelligence>
- 11) 駅構内カメラ画像配信 “駅視 - vision (エキシビジョン)” の実証実験を開始します <http://www.tokyu.co.jp/company/news/list/?id=2392>
- 12) Google のモバイルアプリ向け機械学習モデルが iOS/Android 共通で登場 <https://jp.techcrunch.com/2018/05/09/2018-05-08-googles-ml-kit-makes-it-easy-to-add-ai-smart-to-ios-and-android-apps/>
- 13) FW グループ、EV 向け全固体電池を量産へ <https://response.jp/article/2018/06/22/311132.html>
- 14) UnderWare: Aesthetic, Expressive, and Functional On-Skin Technologies <http://underware.media.mit.edu>
- 15) Cisco、「フォグコンピューティング」 https://www.cisco.com/c/m/ja_jp/solutions/internet-of-things/iot-system-fog-computing.html
- 16) <https://www.iiconsortium.org/>
- 17) トヨタの e-palette 構想 <https://newsroom.toyota.co.jp/jp/corporate/20508200.html>
- 18) 東京大学、医療・介護記録を自身で管理する仕組みを試験運用 <http://techon.nikkeibp.co.jp/atcl/news/15/090400176/?ST=health>
- 19) あいおいニッセイ同和損保、走行距離連動の保険を 4 月から販売…トヨタ T-Connect 活用 <http://e-nenpi.com/article/detail/243935>
- 20) 加古川市、見守り事業開始 <http://www.city.kakogawa.lg.jp/soshikikarasagasu/kyodo/shiminseikatsuanshinka/ICT/mimamori.html>

- 21) ポストムーアの法則時代のコンピューティング
https://www.publickey1.jp/blog/16/qcon_tokyo_2016_3.html
- 22) <http://www.iotac.jp/>
- 23) <https://smartiot-forum.jp/>
- 24) <http://www.onem2m.org/>
- 25) <https://openconnectivity.org/>
- 26) <https://aecc.org/>
- 27) <http://en.econsortium.org/>

2.4.7 ブロックチェーン

(1) 研究開発領域の定義

ブロックチェーンは、ネットワーク上に「ブロック」と呼ばれるデータのかたまりを「鎖(チェーン)」のように連結していく分散台帳の一つの形態であり、仮想通貨ビットコインの実装で初めて用いられた。一般に、分散台帳とは、ネットワーク上の複数のノード間で共有されつつ同期されることで同じ状態が保たれるデータの集合である。整合性を保つために P2P (Peer to Peer) ネットワーク技術と合意形成アルゴリズムが使われる。ビットコインでは、信頼できる第三者機関が存在しない状況でも、個々のデータと系全体のデータの真正性を保証することができるよう高度な暗号技術を採用している。ブロックチェーンに関する基礎から応用まで様々な研究開発が世界中で行われており、ブロックチェーンそのものの実態も今後変化する可能性が高いため、本項では現在および将来にわたってブロックチェーンを構成する可能性のある技術を含め広く俯瞰することとする。

(2) キーワード

分散台帳、公開鍵暗号、ハッシュ関数、P2P ネットワーク、合意形成、インセンティブメカニズム、スマートコントラクト、仮想通貨、ビットコイン

(3) 研究開発領域の概要

[本領域の意義]

ブロックチェーンはその生い立ちから仮想通貨ビットコインとの関係が特に深い。ビットコインはブロックチェーン技術に基づく仮想通貨であり、2008年に Satoshi Nakamoto 論文¹⁾によるアイデアの発表があり、翌年にビットコインのソフトウェアが公開された。これは、暗号技術、P2P (Peer to Peer) ネットワーク技術、分散合意形成技術および継続的運用のためのインセンティブの仕組みから成り立ち、仮想通貨ビットコインの基礎となった。ブロックチェーン技術は、仮想通貨はもとよりそれ以外への適用が期待されており、さまざまな分野で新たなサービスの開発や実証実験が進められている。

ブロックチェーンは、非中央集権的な仕組みで価値の交換を記した台帳を分散共有することを可能にしたことに本質がある。これまで、たとえば銀行が担ってきた「信頼」を中央集権的な組織なしで、安全に共有することができる。すなわち、人と人をデジタル技術に基づく信頼によって結ぶことができるようになったともいえる。中央集権的に保証や仲介をしてきた事業者は不要になり、これまでと違った、分散と自動化による新たなビジネスが可能になる。紙をベースとした仕事の進め方から、完全にデジタルなビジネスへの移行であり、大きな社会変革の可能性を秘めている。

一方で、科学技術的な課題は山積しており、プログラムによる自動取引(スマートコントラクト)などの機能的要件に加えて、性能、安全性などの非機能的要件も改良、改善が必要である。また、金融取引にとどまらず、有形無形資産の取引、デジタルコンテンツの流通、保険や身分の証明など、さまざまな応用に対応するためには、サービス全体の設計・実装基準などの整備も必要である。さらに、これまでとはスキームの異なるビジネスとなることを勘案すると、従来の商習慣や法制度との兼ね合い、それらの刷新も含めて社会との共創が重要なテーマとな

る。さらに、ブロックチェーン技術により実現されている4つの主要仮想通貨システム（ビットコイン、イーサリアム、ライトコイン、モネロ）で使用されているマイニングにかかる消費電力が年間約16.6テラワット時にもなり、スロヴェニアの電力量と同程度といった莫大な電力消費量となっており、世界の電力消費への脅威だけでなく、地球環境への影響についても喫緊の改善が必要である²⁾。これらの課題を解決し続けることによって、ブロックチェーン技術は新しい法、経済、社会制度を生み出す基盤となることができる。

【研究の経緯】

ブロックチェーンに関わる技術の系譜をたどる。ブロックチェーンは仮想通貨ビットコインを実現するために設計された。仮想通貨自体は暗号技術の応用として古くから考えられてきた。David Chaumのブラインド署名技術を用いたDigiCash³⁾は暗号技術に基づく仮想通貨の草分けである。DigiCashはさまざまな理由から普及には至らなかったが、2008年にSatoshi Nakamotoが書いた論文とその実装により、ビットコインが生まれた。当初のブロックチェーンは、ビットコインの実現に特化して設計された、暗号技術とP2Pネットワーク技術、分散合意形成技術などの既存技術の統合といえる。Satoshi Nakamotoの功績は、通貨の発行をProof of Workと呼ばれる分散台帳の整合性維持に対する作業への対価とすることで、継続的に運用できるインセンティブメカニズムを考案したことである。本稿では、ビットコインおよびビットコインから派生した仮想通貨（オルトコイン）で使われるブロックチェーン技術を第1世代とする。

ビットコインの成功により、ブロックチェーンに対して、仮想通貨以外にも応用できる技術としての期待が高まり、新たなブロックチェーン技術が研究・実装された。その代表がスマートコントラクトである。スマートコントラクトは、取引情報中にある種のプログラムを組み込むことにより、価値交換以外の情報管理や処理を可能にする仕組みである。たとえば、ある一定の条件を満足した場合に支払いを行うというような契約を自動的に実行することもできる。これを第2世代とする。

ブロックチェーンは汎用的な情報処理の技術基盤であると考えれば、今後、第3世代としてさらに広範な応用が広がるだろう。どのような応用が生まれるのか、そのためにはどんな技術的発展が必要かということは今後の研究開発、ビジネス開発にかかっている。

【研究開発の動向】

プラットフォーム化するブロックチェーン

ビットコインの技術基盤として生まれたブロックチェーンの汎用性を活用した応用が次々に生まれ、また、同時にビットコイン以外のブロックチェーンを処理する実行基盤（プラットフォーム）も登場した。現時点での代表的なプラットフォームとして、ビットコイン、イーサリアム、Hyperledger Fabricがあげられる。次項に述べるように、それぞれ管理者の有無と参加者の参加方法やできることが異なる。イーサリアムは、ビットコインの課題解決や新たな拡張性を目指して全く新規に設計された。独自仮想通貨イーサの執行基盤でもあるが、契約、権利管理等への利用をめざして開発が進められている。Hyperledger Fabricは主に企業でのブロックチェーンの活用を目指してOSS（Open Source Software）プロジェクトとして開発が進められている。表2-4-1にプラットフォームとしてのビットコイン、イーサリアム、Hyperledger Fabricの特徴をまとめた。

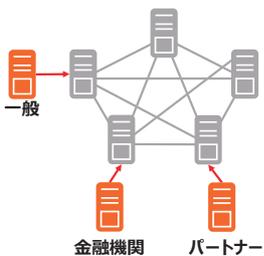
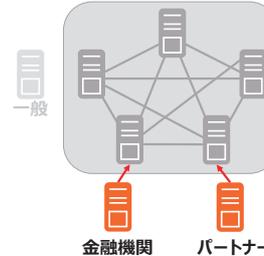
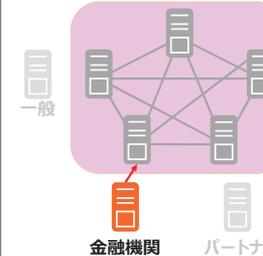
表2-4-1 代表的なブロックチェーン・プラットフォーム

	ビットコイン	イーサリアム	Hyperledger Fabric
開始年	2008	2015	2015
開発主体	Satoshi Nakamoto 他	イーサリアム財団	LINUX、IBM、Intel、ソラミツ他
形態	パブリック型	パブリック型	パブリック型・プライベート型
内容	仮想通貨としての流通	仮想通貨を含めた取引一般	様々なソリューションの技術基盤
合意形成方式	Proof of Work	Proof of Work。 今後 Proof of Stake へ変更予定。	PBFT (v0.6)、 EndorcementPolocy (v1.0)
通貨	BTC (ビットコイン)	ETH (イーサー)	通貨なし/あり
プログラミング	スクリプト (scriptSig) による 限定されたプログラム	スマートコントラクト言語に よる自由なプログラム	スマートコントラクト言語に よる自由なプログラム

パブリック型からプライベート型、コンソーシアム型へ

ビットコインは、管理者に相当する組織が存在せず、誰もが平等で、誰からも許可を得ることなくネットワークに参加できる、非中央集権な P2P ネットワークである。このようなオープンなブロックチェーンはパブリック型やパーミッションレス型と呼ばれる (以下、本項ではパブリック型と呼ぶ)。一方、例えば、米国 Ripple Labs が運営する仮想通貨 Ripple のようなケースでは、管理者がおり、参加できるのは特定の限られた者のみである。このような、中央管理者を置き運営しているブロックチェーンはプライベート型やパーミッションドと呼ばれる (以下、本項ではプライベート型と呼ぶ)。また、プライベート型の派生形で複数の管理者からなるコンソーシアム型もある。これらについて、表 2-4-2 に整理した。

表2-4-2 参加モデルによるプラットフォームの分類

参加モデル	パブリック型	コンソーシアム型	プライベート型
構成			
管理者の有無	なし	あり (複数企業)	あり (単独)
参加者	不特定多数 (Permission less)	特定複数 (Permissioned)	組織内 (Permissioned)
合意形成の仕組み	PoW / PoS (※ 2) など (厳格な承認が必要)	特定者間のコンセンサス (厳格な承認は任意)	組織内承認 (厳格な承認は任意)
参加者のアクセス権	全員がフルアクセス	管理者が決める	管理者が決める
プラットフォーム	ビットコイン (※ 1 BCN) イーサリアム	Hyperledger Fabric	Hyperledger Fabric Ripple

※ 1 BCN: ブロックチェーンネットワーク ※ 2 PoW: Proof of Work / PoS: Proof of Stake

画像: Fujitsu | 金融ソリューション ~ブロックチェーンの取り組み~を参考に作成
(<http://www.fujitsu.com/jp/solutions/industry/financial/concept/blockchain/>)

パブリック型の場合は、参加者の賛同が必要であるため、ブロックチェーンの仕様変更は一般には難しい。合意できない場合は、過去ビットコインで起こったような分裂（フォークという）が発生する。プライベート型の場合は管理者の決定で自由に変更でき、柔軟なシステムの運用が可能である。プライベート型の場合は、新しい技術の検証などがしやすく、企業を中心に、契約、取引そのほかの実証実験のベースになっていることが多い。

このように、「完全に自律分散的なブロックチェーン」と「中央管理に適したブロックチェーン」という全く異なる性格が表れる。パブリック型ブロックチェーンは、そもそも中央集権機関などの既存の枠組みとは根本的に相容れないモデルであり、既存の枠組みを破壊しながら発展し普及する可能性もある。この結果、将来的には分散化による完全な仲介者の排除が実現されるかもしれない。一方でパブリック型ブロックチェーンには合意形成に時間がかかる等の現実的な課題があるため、それを解決する一つ的手段としてプライベート型のブロックチェーンが考案された。プライベート型ブロックチェーンは、既存の枠組みを大きく変えずに効率化を進めることができるため、企業や銀行等におけるプライベート型ブロックチェーンの採用が今後急激に進む可能性もある。

仮想通貨以外への応用

ブロックチェーンは、もともとビットコインのために発明された技術であるが、通貨以外への応用としては、金融取引、資金調達（ICO）、不動産取引、電力取引、投票などがあり、改ざんが難しいという特徴を利用して、身分証明、土地の登記簿、選挙の投票の仕組み、ダイヤモンドの認定書と取引履歴の記録簿、不動産情報管理システムなどの応用例もある。詳細は(4)注目動向に記載。

【標準化の状況】

ISO では 2016 年 9 月 に ISO/TC307 Block-chain and electronic distributed ledger technologies を設置し、ブロックチェーンと電子分散台帳におけるシステム、アプリケーション、ユーザー間の互換性やデータ交換にかかわる国際標準化活動を開始した。2018 年 10 月時点で 39 か国が参加し（他に 13 か国のオブザーバ）作業中である。

(4) 注目動向

【新展開・技術トピックス】

スマートコントラクト^{4, 5, 6)}

スマートコントラクトは「契約の締結と実行の自動化」であり、1994 年に Nick Szabo という法学者・暗号学者により提唱された。本項ではブロックチェーン上であらかじめ設定していたプログラムにより自動的にトラスレス（信用を考慮する必要がないこと）で取引を実行する仕組みを指す。ビットコインの使用言語（スクリプト）は分岐やループを持たないため、実行できる処理は限定される。一方で、イーサリアムは自由なスマートコントラクトを書くためのチューリング完全と呼ばれるプログラム言語を提供、さまざまな契約を仲介者無しで自動的に実行するためのプログラムが作成できる。例えば、車の購入を考えてみる。売り手はスマートフォンなどの電子鍵で車のカギをロックできるとする。スマートコントラクトにより買い手が契約条件通りの金額を支払うと、そのイベントを検知して自動的に車の所有権とカギを購入

者に移転し、それにより買い手のスマートフォンなどの電子鍵で解錠可能となり、すぐに運転ができるようになる。このように一定の取引条件を満たしたことを確認して契約を自動的に執行できる仕組みが可能になる。しかし、実際にスマートコントラクトが機能するためには、取引条件を満たしていることを現実世界にアクセスして保証する信頼できる第三者（オラクルと呼ばれる）が必要となる。

DAG（有向非巡回グラフ：Directed Acyclic Graph）^{7,8,9)}

ブロックチェーンは基本的に複数の取引（トランザクション）をブロックとしてまとめて、それをチェーン状につなぐ構造を持つが、DAG は一つ一つの各取引をユニットとして巡回しないよう一方に複数のチェーンでつなげた構造を持つ。DAG では取引をまとめたブロック生成が不要なので、その報酬を目的とした Proof of Work の概念がない。DAG を用いた分散台帳には、2016 年に公開された仮想通貨 IOTA、Byeball などがある。IOTA では DAG を用いた Tangle と呼ばれる技術を用いており、取引を行う自分自身が過去の二つの取引を承認しながら DAG への組み込みを行う。一定時間内に多くの取引を取り込めるとともに、パブリック型の課題とされるインセンティブ不整合（ブロックチェーンの承認機能を支えるマイナーのインセンティブは報酬であり、取引台帳の維持ではないこと。このため報酬の低下がブロックチェーン自体の機能不全を引き起こす）が回避でき、手数料が掛からない高速な取引が実現できる。このように IOTA は、名前の由来通り IoT におけるマイクロペイメントと呼ばれる少額取引に特化した仕組みになっている。ただし DAG を用いた分散台帳技術は歴史が浅く、セキュリティ、信頼性等についてはまだ十分検証されているとは言えない。

ビットコイン・ブロックチェーンを用いたオフチェーン技術

ビットコイン・ブロックチェーンを少額取引（マイクロペイメント）として利用する場合、手数料が高いことや取引のスループットが低い（約 7 取引 / 秒）という課題がある。この問題を解決するために基盤レイヤー（レイヤー 1）となるビットコイン・ブロックチェーンの外に、レイヤー 2 として新しいシステムを設けることで対応するオフチェーン技術が検討されている。有名なものとしてはライトニングネットワークがある。すでにいくつかの実装プロジェクトが進んでいるが、開発途上であり、実現にはビットコイン本体の仕様変更を必要とする。しかし、将来的にビットコインのスケーラビリティの問題を解決し、多様な用途でマイクロペイメントを実現できると期待される。

[注目すべき国内外のプロジェクト]

本項では主に応用に向けた取組みを紹介する。

FinTech × ブロックチェーン

日本銀行は欧州中央銀行と共同で、Project Stella を 2015 年から進めている¹⁰⁾。これは、金融市場インフラへの分散型台帳技術の応用可能性を調査するものである。このプロジェクトは、技術に関する概念的な整理（法的な議論を除く）だけでなく、実際に実験を行いながら進められている。現在、調査の途中であるが、Hyperledger 基盤を用いた検討の結果を踏まえ、分散型台帳環境下での証券と資金の受渡が実現できることを明らかにしている。分散

型台帳を応用して DvP (Delivery versus Payment) を実現するといった議論は始まったばかりであり、これらのアプローチの安全性や効率性について、さらなる分析が必要であることも指摘している。

電力取引×ブロックチェーン

日本でのフィードインタリフ制度 (固定価格買取制度) の導入を契機に、蓄電池や分散型電源、再生エネルギーの普及を促進するため、新たな電力取引の仕組みを考える動きが出てきた。分散型電源を利用し「地産地消」を図るコンセプトは従来からあったが、関連技術の進展により取引システムが安価に構築可能になったことから、ブロックチェーンの利用を含め検討が加速している。多くは電力取引システムへの応用であるが、一步踏み込んだ非同期連系技術の検証を行っている事例を紹介する。東京大学はメーカー・電力会社などと提携し、さいたま市美園地区(みそのウィングシティ)で電力取引システムの検証実験を 2017 年から始めた。これは、DGR (デジタルグリッドルータ: 系統に接続する電力変換器がそれぞれ固有のアドレスを持ち、ブロックチェーンを介して取引し、電力ルーターを同時に動作させる) を用いた電力潮流制御を用いた仕組みである。太陽光発電、蓄電池の電力を株式市場のようなザラ場で価格を決め、売りと買いの約定が成立したもの (同時同量) のみが流れるようになっており、引き取り手がない電気は入れないようにしている。このため系統への負担を抑えられる。この技術により電力は通信におけるパケットのように取り扱われる。

医療・ヘルスケア×ブロックチェーン

ブロックチェーンが、医療・ヘルスケアに徐々に浸透しつつある。世界最大のヘルスケア IT の国際会議・展示会である HIMSS : Healthcare Information and Management Systems Society において 2018 年次総会以後、ブロックチェーンが主要セッションの 1 つとして大きく取り上げられている。また、エストニアのように国を挙げて医療・ヘルスケアにおけるブロックチェーンを実践する事例も存在する。

しかし、わが国では実際に当該領域に取り組む研究者は、アカデミア、企業とも極めて少ないのが実態である。2018 年 9 月時点で、「医療・ヘルスケア×ブロックチェーン」を研究実施対象と明言した唯一のプロジェクトが、戦略的イノベーション創造プログラム (SIP) 「AI (人工知能) ホスピタルによる高度診断・治療システム」である。同プロジェクトの研究開発計画書 (平成 30 年 7 月 19 日) では「サブテーマ A : セキュリティの高い医療情報データベースの構築とそれらを利用した医療有用情報の抽出、解析技術等の開発」の中に、「⑦トレーサビリティ、スマートコントラクトを内包するブロックチェーン技術等を応用した通信プロトコルの開発」が公募対象として掲げられている¹¹⁾。わが国の医療・ヘルスケアにブロックチェーン技術を実装するために検討すべき課題は多いが、ブロックチェーンは、そのような状況に大きな風穴をあける、破壊的な技術としてのポテンシャルを有すると期待されている。

【諸外国の政策や海外動向】

エストニア～ブロックチェーン先進国～^{12), 13)}

人口 132 万人 (2018 年) の小国であるエストニアは、国を挙げて電子政府化に取り組んでいるデジタル先進国である。ブロックチェーンにおいても先進的なチャレンジを続けており、

ビットコインの登場よりも早い2008年に、ブロックチェーンの原型とも言える“hash-linked time-stamping”技術の試験的実装を開始した。2012年には正式に実装され、エストニアは世界初のブロックチェーン導入国家となった。

エストニアにおけるブロックチェーン導入と深く関係しているのが、2006年に同国に設立されたGuardtime社である。同社は、Keyless Signatures Infrastructure (KSI)¹⁴⁾という独自のブロックチェーン技術を強みとしている。従来のブロックチェーン技術は公開鍵暗号方式を採用してきたが、KSIはハッシュを台帳の維持管理にのみ利用している点に特徴がある。KSIはブロックチェーンのもつ改ざん耐性をもちつつ、限られた機関でのみ利用可能とした技術であり、例えば医療情報のような高度な個人情報をも有するデータも取り扱い可能である。KSIブロックチェーン技術は、e-ヘルスレコード、e-処方箋データベース、e-Law / e-Court システム、e-Police データ、e-バンキング、e-ビジネス登録、e-Land などのエストニア電子政府の多くのサービスを保護している。また、タリン工科大学 (Tallinn University of Technology) では、e-ヘルス実現のために、すべての医療データの完全性をブロックチェーン技術によって保証する研究が進められている^{15, 16)}。

EU Blockchain Initiative

EUはBlockchain Initiativeとして複数のプロジェクトを平行して走らせている。2018年2月には、ブロックチェーンによるイノベーションの加速とEU内のブロックチェーンエコシステムの開発を目的としたEU Blockchain Observatory and Forumを設立した。100名規模の有識者によるフォーラム活動を精力的に実施し、“Blockchain Innovation in Europe”、“Blockchain and the GDPR”、“Blockchain for Government and Public Services”等の質の高いレポートを発行している¹⁷⁾。Digital Single Marketも2017年の中間評価でブロックチェーンに関連づけられた。他にも、“Horizon Prize on Blockchains for Social Good”や仮想通貨に関するプロジェクトもイニシアティブの下で開発が進められている。

BSafe.network

ビットコインは当初個人や企業を中心に開発がなされ大学等の研究機関の関与はあまり見られなかった。不安を抱えながら動作しているのが現状である。そこで、ブロックチェーン技術の不安を解消し、誰からも信頼できる技術とすべく、2016年、BSafe.networkがMITからの呼びかけに応じて設立された。これは研究用のブロックチェーン専用のネットワークである。世界中から日本(東大、慶大、東邦大、立命館大、早大が参加)を含むアジア、ヨーロッパ、北米、そしてアフリカの28の大学が参加している。参加するとネットワークのノードが置かれ、研究成果を実装したソフトウェアをインストールして実行することで、研究成果の有効性を確認できる。このプロジェクトでは、セキュリティ、ネットワーク技術、コンセンサスメカニズム、ゲーム理論、経済学、および規制に関わることなど、ブロックチェーンに関わるあらゆる要素が研究と実験の対象になっている。インターネットのための技術開発を行う際にNSFNetが果たしたのと同じ役割を担うことを想定している。

米国 IEEE (Institute of Electrical and Electronics Engineers)

米国IEEEは、ブロックチェーン技術の開発と採用において重要な役割を果たすことを考え

ており、2018年1月にIEEE Blockchain イニシアチブ (BCI) を発足させた。BCIはIEEEにおけるブロックチェーンの全てのプロジェクトおよび活動のベースとなる。BCIは、標準化、教育、イベント、コミュニティ開発とアウトリーチなどといった様々な活動で構成されている。また、BCI発足後最初のシンポジウムを2018年7月にBlockchain-2018: The 2018 IEEE International Conference on Blockchainとして開催した。

Ripple社「大学ブロックチェーンリサーチ構想 (University Blockchain Research Initiative: UBRI)」プロジェクト

2018年6月、Ripple社は、「大学ブロックチェーンリサーチ構想UBRIプロジェクトについて、選抜した世界有力17大学と共同提携すると発表した。プロジェクト全体の寄付金総額は、5千万ドル(約55億円)であり、同社の持つ専門知識や技術的資源の提供を受けながら、ブロックチェーン、仮想通貨と電子決済等に関する学術研究を行なう計画である。選抜した17大学の内訳には、中国や日本は含まれておらず、米国の7大学(MIT コンピューター科学AI研究所、Princeton 大学情報技術政策センター、UCB ハースビジネススクール、Texas 大学 Austin 校マコームズビジネススクール、Oregon 大学、Pennsylvania 大学、North Carolina 大学 Chapel Hill 校)、欧州の4大学(英国・University College London (UCL)、オランダ・Delft 工科大学、ルクセンブルグ・Luxembourg 大学、キプロス・Nicosia 大学)、インドの2大学(インド情報技術大学ハイデラバド校、インド工科大学ボンベイ校)、カナダ・ウォータールー大学、オーストラリア・オーストラリア国立大学、ブラジル・ジェットウーリオ・ヴァルガス財団、韓国・高麗大学の17大学である。また、Ripple社は、中国・清華大学金融科学技術研究所 (THUIFR) との提携を別途結び、大学院生を対象としたブロックチェーン技術研究奨学金プログラム (BRSP) を2019年1月から開始している。ブロックチェーン業界の未来を担う若い人材のために、ブロックチェーンに関する国際的な規制についての認識を広め、ブロックチェーン技術の研究機会を提供することを目的としている。

その他の注目動向

Shawn Fanning (音楽ファイル共有ソフトNapsterの開発者)らが創業した米国IoTスタートアップHeliumは、ブロックチェーンの仕組みを利用して、安価でどこでも利用可能なIoTデバイス向けのネットワーク網を新たに構築するための研究開発を行っている。彼らが開発するシステムは、「Proof of Coverage」と名付けられ、低消費電力ゲートウェイが分散型元帳を管理するためのマイナー的な役目を担う。

また、Matthew Spokeが創業した米国スタートアップAionは、ブロックチェーンの相互運用のための「token bridge (トークン・ブリッジ)」を開発し、イーサリアムベースのトークン保有者が、Aionのブロックチェーン上に資産を実際に移動することなくバックアップする実証実験を行っている。

(5) 科学技術的課題

ブロックチェーンに関わる技術全体を俯瞰する(図2-4-3)。最下層は、ブロックチェーンが依拠する技術(暗号技術、P2Pネットワーク、分散合意形成)であり、計算機科学の分野においてそれぞれ30年以上の歴史を持つ。その上に位置するのは、ブロックチェーンをブロック

チェーンたらしめる固有技術（分散台帳、スマートコントラクト、システム運用管理）である。また、これらの技術を使って特定の応用を効率的に実現するための実行環境を応用分野との間に定義した。ソフトウェアとしてのプラットフォームと制度設計や信用モデルから成る。

ブロックチェーンの応用は、ブロックチェーン上に記録されるデータの種類の、取引管理と情報共有・情報管理の2つに分けられる。取引管理は、複数の当事者間のやり取りの記録を管理し、情報共有・情報管理は、特に取引に関わらない種々の情報の記録を管理する。情報共有と情報管理の違いは、一般に記録された情報を公開情報として扱うか、個人情報として扱うかの違いであるが、厳密には決められないものもあるため、ここではまとめて扱う。



図2-4-3 ブロックチェーン技術の俯瞰

以下、個々の技術的課題について列挙する。

[ブロックチェーン固有技術]

分散台帳：ファイナリティ、スケーラビリティ、匿名性

仮想通貨に用いられるパブリック型においては、ブロックに格納されるトランザクションの真正性を確定することをファイナリティと呼ぶ。P2P ネットワーク上で異なるマイニングノードが異なる時間関係で受信したトランザクション情報をもとに新規ブロック候補を作成するので、本来同一のブロックチェーンを分散して持つべきなのに、各マイニングノード間で新規ブロックの内容に差異が出ることは避けられない。ビットコインでは、新規ブロック候補に、さらに新たなブロックが6個つながったら当該ブロックが確定したものとみなしているが、これは確率的

な判断であり、絶対的な確定とは言えない。このため、ビットコインの場合、ブロックサイズ (1 MB)、トランザクションの平均サイズ (300B)、ブロック生成時間 (約 10 分) から、7 トランザクション/秒がその性能限界といわれる。一般に、クレジット決済などの処理能力は数千トランザクション/秒以上を処理できるため、それと比較してあまりに貧弱な性能しか確保できないことをスケーラビリティ問題と呼ぶ。ビットコインにおいても、ライトニングネットワーク (レイヤ 2 技術の一種) を用いてこの課題を解決しようとしているが、まだ実験検証の段階である。分散台帳に関する三つ目の課題が、匿名性・プライバシーの問題である。ビットコインでは、ユーザーの ID として公開鍵暗号の公開鍵のハッシュ値を用いることによってユーザーの実名は秘匿している。トランザクションは公開されているため他の情報と突合することでユーザーを特定することが可能である。また、そもそも取引内容を公開したくない場合も多い。

スマートコントラクト：プログラミングモデル、プログラミング言語、正当性検証

スマートコントラクトに関してはシステムとして採用すべきプログラミングモデルの選択といかなるプログラミング言語を実装すべきかが課題となる。ビットコインではスクリプト型のプログラミングを用いて簡単な取引処理が記述可能だが、分岐やループ処理が行えずその記述範囲には限界がある。そこで、イーサリアムではチューリング完全型のプログラミング言語 (Solidity) を実装したが、チューリング完全性ゆえにその結果がユーザーの意図したものか否かの検証 (正当性検証) に課題がある。また、自由度が高い分、ハッカーに攻撃される可能性も高くなる (DAO 事件がその例)。

システム運用管理：鍵管理、版管理

そもそもビットコインは仮想通貨の発行と支払いまでを対象としていたがため、法定通貨との交換や仮想通貨以外の応用に関しては考慮がない。したがって、ビットコインのために発明されたブロックチェーンを今後、広く社会システムの基盤の一部として機能させせるためには、例えば、一般の利用者の使用を前提とした交換所や取引所などのシステムを想定した機能や非機能要件を満たす必要がある。具体的には、ユーザーの ID 管理、鍵管理 (有効期限、更新、失効) やブロックチェーンネットワークのソフトウェアの版管理など、信頼できる機関による管理を前提とせざるを得ない場合もある。

[ブロックチェーンが依拠する基盤技術]

暗号技術の危殆化：量子コンピューター、暗号プロトコル

ブロックチェーンの各ノードから発信されるトランザクションの耐改ざん性はハッシュ技術によって担保されており、発信者の正当性は電子署名によって検証される。ビットコインをはじめとする仮想通貨では、現時点での暗号解読技術・能力に耐えるように、ハッシュ関数、署名方式が選択されている (ビットコインではハッシュ関数として SHA-256 と RIPEMD160 が使われ、公開鍵暗号としては secp256k1 (楕円曲線暗号の一種) が使われている) が、将来の暗号解読能力の進歩、例えば、量子コンピューターによって、これらの暗号技術が破られる危険性がある (危殆化)。暗号技術の危殆化に対しては、新たなハッシュ関数、署名方式の開発など暗号技術そのものの研究と、すでに動いているブロックチェーンの内容を新方式に安全に移行する仕組みに関する研究の両方の側面がある。

P2P ネットワーク：可用性維持、攻撃耐性

ブロックチェーンの各ノード間の通信には P2P ネットワークが用いられる。この P2P ネットワークにおける通信経路（各ノードが他のどのノードと通信するかのネットワーク構成）が、分散合意形成におけるマイニングノード間の公平性に影響を与える可能性がある。マイニングに参加するノード間で公平な条件になるような P2P ネットワークの構成が課題となる。また、DOS 攻撃や DNS ハッキングのような手法で、P2P ネットワークが歪められて、分散合意形成が機能しなくなる可能性があるため、これらの対策も必要である。

分散合意形成：合意形成アルゴリズム、インセンティブ設計、攻撃耐性

パブリック型においては、複数のトランザクションをまとめて新たなブロックを作成する際に、どのトランザクションを真正なトランザクションとして認めるかという、多くのノードによって分散的に行われる合意形成が必要になる。ビットコインにおいては、この検証作業への報酬として、最初に成功した作業者にブロックに追加する権限と併せて新規仮想通貨を与えることとしている（Proof of Work）。この作業には多大な計算機パワーを必要とし、電力消費が問題となっている。イーサリアムなどの仮想通貨では、この点を解決するために合意形成の決定権を多くの通貨を持つノードにより多く与えるという別の分散合意形成アルゴリズム（Proof of Stake）が提案されているが、そのインセンティブの設計を含め実効性の検証は今後の課題である。

（6）その他の課題

ブロックチェーンはビットコインの成功により仮想通貨への応用が注目されがちだが、改ざん困難な分散台帳の応用は、取引管理だけでなく情報共有・情報管理まで広範である。現状は、ブロックチェーンは、情報だけでなく価値交換の基盤から社会基盤そのものになる可能性があるとして将来性を期待する声は大きい。しかし、現実には仮想通貨以外の応用に関しては、ブロックチェーンを使わなくても実現できるケース（Blockchain Inspired Solution と呼ばれる）も多く、新たな応用の開拓に苦慮している。

根本的な原因は、ブロックチェーンが基盤技術も応用技術も未熟なことにある。投機的な価値を持つ仮想通貨をとにかく獲得するためのエンジニアリング技術、特にマイニング技術の進化は専用の ASIC を開発するまでに至る。一方で、すでに見たように科学技術的な課題も山積している。そもそもブロックチェーンは総合格闘技と呼ばれることがあるように、構成する要素技術は、暗号技術・P2P ネットワーク・分散合意形成、社会システムデザインなど、これまで相互に交わる機会があまりなかった研究コミュニティに属する。ブロックチェーンを将来の社会インフラ技術の重要コンポーネントとするために、準備段階として研究開発や社会実装の環境整備が必要である。以下にそれらの課題のうち特に重要と考えるものを記述する。

インキュベーション・プラットフォームによる人材育成とキラーアプリの創出

ブロックチェーンの現状は 1990 年代のインターネットに似ていると言われる。電子メールが使われ始め、ブラウザや HTTP サーバーによる WWW の実装が始まったころ、我が国では WIDE プロジェクトとして大学や研究機関などを対象とした非営利目的のインターネット利用技術の開発が行われた。その後、インターネットの商用利用が始まり、新たなアイデアをもっ

たベンチャー企業が登場し、グローバルな情報処理・情報通信のインフラとしての基盤が成立した。30年前とは環境がまったく違うため同じアプローチが成功するとは思えないが、多種多様な動機や興味をもった人材が、さまざまなアイデアを試行しお互いに切磋琢磨する「るつぼ」のような環境が必要である。人材が生まれ次世代のキラアプリが生まれ始めるのにある程度、例えば5年から10年程度の、時間がかかることを考えると待ったなしの状況であると言える。

法制度とシステム開発のコ・デザインによる社会システムの再構築

経産省がとりまとめた「ブロックチェーン技術を利用したサービスに関する国内外動向調査」¹⁸⁾では、ブロックチェーンが起こす社会変革の可能性として、地域通貨、土地等の登記、C2C (個人間) 取引、開かれたサプライチェーン、取引の自動化などを具体例として挙げているが、いずれも既存の法規制や商習慣の枠組みを逸脱する可能性が高い。このような新たな社会システムを構築するためには、設計の段階から法制度の再設計とシステムの開発とを同時にデザインすることが不可欠である。

持続的に運用できる仕組みの創出

ブロックチェーンをつかって再構築された新たな社会システムにおいては、ブロックを生成するインセンティブを確保し続けることが課題となる。分散合意形成がPoW等ではうまくいかない場合には、例えば、PoA (Proof of Authority) のような別の仕組みが必要となり、その際にはオーソリティとしての国や自治体などの存在が改めて重要となる。エストニアなどの取り組みを参考にした施策の検討が望まれる。

(7) 国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	<ul style="list-style-type: none"> 慶應義塾大学の大槻知明教授らのグループは、ブロックチェーン技術を応用し、製品が消費者の手に渡った後も偽物製品の検知が可能な所有権管理システム (POMS: Product Ownership Management System) のプロトタイプを開発し、2017年7月に発表¹⁹⁾。 慶應義塾大学の松谷宏紀准教授らのグループは、GPUを用いたブロックチェーンキャッシングによる取引の異常検知に関する研究成果を2018年12月にIEEE国際会議ISPA 2018で発表²⁰⁾。
	応用研究・開発	○	→	<ul style="list-style-type: none"> トヨタとToyota Research Institute (TRI) は2017年5月、自動運転車の開発に使う走行データの取引市場やカーシェアリングの運用などに、ブロックチェーン技術の適用を検討すると発表。トヨタは研究所に対して、2016年～2020年の5年間にかけて約10億ドル (約1,120億円) を投入する予定。 2018年2月、NECおよびNEC欧州研究所は、取引記録に参加するノード数200ノード程度の大規模接続環境下で毎秒10万件以上の記録性能を達成する世界最速のブロックチェーン向け合意形成アルゴリズムを開発し、世界規模のクレジットカード取引を支えるシステムとして必要とされる毎秒数万件を超える性能を実現。 富士通は、2017年11月、ブロックチェーン同士を安全につなげるセキュリティ技術「コネクションチェーン」を開発。また、同社は2018年3月、ブロックチェーン研究開発の拠点として、ブロックチェーン・イノベーション・センターをベルギー・ブリュッセルに開設し、ベルギーにおけるスマートシティの実現に向け、ブロックチェーンの利用を検討開始。

米国	基礎研究	◎	→	<ul style="list-style-type: none"> UCB の Dawn Song 教授らの研究グループは、Ethereum の根本的な制約を克服する新たな「プライバシーを重視した」スマートコントラクト技術を探求。 MIT の Thomas Hardjono 教授らの研究グループは、データグラム (ネットワーク間を行き来できる情報の共通単位) と呼ばれるインターネット・プロトコル・スイートの概念を提案し、現在のブロックチェーン開発者はデータグラムの概念を取り入れるべきだと主張。
	応用研究・開発	◎	→	<ul style="list-style-type: none"> Microsoft は、Azure 上で動作する BaaS (Blockchain as a Service) の開発・展開に加え、分散台帳技術を開発するエンジニアに向けて新たに Azure Blockchain Workbench を公開した。 Google は、ブロックチェーンを用いて改変を検知できるログに署名を保管し、システムに保管された情報が修正されていないことを保証するか、何の情報がいつ変更されたかを追跡可能とする技術に関する特許を 2017 年 9 月に申請した。Google がブロックチェーン技術を用いた情報保護を模索していると推察されている。 UCB の Dawn Song 教授は、研究成果を基にスタートアップ Oasis Labs を創業し、暗号通貨専門ファンド Andreessen Horowitz から 3 億ドルの出資を受けた。また、プライベート・トークンの先行販売により、投資家達から 4500 万ドルを調達している。Oasis Labs は、開発した「プライバシーを重視した」スマートコントラクト技術を用いて、スマートコントラクトの実行をブロックチェーンの合意形成から切り離すことで、データへの選択的アクセス許可と確実な機密保持の 2 つを提供することを目指している。 ベリディウム基金 (Veridium Foundation) は IBM と提携して、公開型の Stellar ブロックチェーンを使って、「二酸化炭素排出権 (炭素クレジット) のトークン化」を計画している (2018 年後半発行予定)。これは、IBM にとっては、公開型ブロックチェーンと許可型ブロックチェーンとを組み合わせる実証実験であり、炭素クレジットを他の商取引と組み合わせる実証実験でもある。
欧州	基礎研究	○	→	<ul style="list-style-type: none"> Wien 工科大学の Matteo Maffei 教授が率いる研究グループが、Ethertrust プロジェクトにより、Ethereum のスマートコントラクトのセキュリティを向上させる研究成果を 2017 年 11 月末に発表。 スウェーデンのチャルマース工科大学 (Chalmers University of Technology) では、公平なモビリティサービスに向けた MaaS (Mobility as a Service) におけるブロックチェーン技術の役割について研究している。 フィンランドの Aalto 大学は、Pekka Nikander 教授をリーダーとして、2018 年から SOFIE と呼ばれる 3 年間の EU Horizon 2020 プロジェクトを立ち上げ、技術的および商業的にオープンなフレームワークを創造し、IoT を統合するためのオープンなビジネスプラットフォームの創出に関する研究を行っている。
	応用研究・開発	◎	↗	<ul style="list-style-type: none"> IoT のための仮想通貨 IOTA と有向非巡回グラフを応用した IOTA のコア技術 Tangle に関するプロジェクトが、ベルリンを拠点にして 2015 年に始まった。 EU の DECODE (Decentralised Citizens Owned Data Ecosystem : 分散型市民所有データエコシステム) プロジェクトが、2017 年に開始。個人データを米国大手 IT 企業から取り戻し、データ主権を個人にもたらしことを目的としている。現在、EU Horizon 2020 プロジェクトの一環として、14 のコンソーシアムメンバーに総額 500 万ユーロ (約 6 億円) の資金が 2019 年末まで提供され、プロジェクトが進行中。分散型台帳技術と組み合わせる DECODE の新技術は、アムステルダムとバルセロナで実証実験が行われる予定。 My Health My Data (MHMD) プロジェクトは、医療データのプライバシーとセキュリティにおける新しいパラダイムシフトを目指した EU Horizon 2020 プロジェクトであり、2016 年 11 月にスタートした。EU から総額 400 万ユーロ (約 5 億円) の資金が 2019 年末まで提供され、機密データとしての医療データの共有方法を根本的に変えることを目指している。 フランスの銀行グループ Société Générale とオランダの金融サービス会社 ING が協力して、石油取引に焦点を当てた Easy Trading Connect プロジェクトとして、ブロックチェーン技術の導入により商品取引の処理時間を 3 時間から 30 分未満に短縮できることを 2017 年 2 月に実証した。 デンマークのコペンハーゲンに本社を置く海運業界のスタートアップ Blockshipping は、世界中の 2700 万個のコンテナをリアルタイムで追跡、記録する世界初のブロックチェーン・プラットフォーム (Global Shared Container Platform: GSCP) を開発中。 オランダ最大級のスーパーマーケットチェーン Albert Heijn は、2018 年 9 月、清涼飲料水を専門とする充填事業者 Refresco と提携して、プライベートブランドのオレンジジュースを対象に、ブロックチェーン技術を活用して、ブラジルのオレンジ農園から各店舗に陳列されるまでのサプライチェーンをすべてデータ化することで、サプライチェーンの透明化を開始。

中国	基礎研究	○	→	<ul style="list-style-type: none"> 清華大学 Li Liao 教授らは、世界初のパーソナル AI 技術を開発しているベンチャー企業 ObEN とともに、ブロックチェーンの多くの課題（セキュリティ、トランザクション速度、容量、スケーラビリティ、およびエコシステム構築）を探索している。
	応用研究・開発	◎	↗	<ul style="list-style-type: none"> 中国初のブロックチェーン実験特区が 2018 年 10 月、海南省海口市に正式にオープン。仮想通貨取引所 Huobi（火幣）は、国内本社を移し、Tianya Community（天涯社区）とともにブロックチェーン研究室を設立するとともに、10 億ドル規模のグローバルブロックチェーン業界ファンドを創設する計画。 Alibaba（阿里巴巴）が提供するクラウドサービス Alibaba Cloud's BaaS の提供地域が、2018 年 10 月、米国、ヨーロッパ、東南アジアなどを含む国際市場にまで拡大。なお、本技術は、Hyperledger Fabric に加え、Ant Blockchain（Alibaba グループの金融関連会社 Ant Financial Services が独自開発した Blockchain プラットフォーム）に基づいたものである。 Web サービス会社 JD.com（京東商城）は、米国 New Jersey 工科大学と中国科学院ソフトウェア研究所（ISCAS）と協力してブロックチェーン研究所を 2018 年 10 月に設立。分散型アプリケーション（DApps）の基本的なコンセンサス・プロトコル、プライバシー保護、セキュリティなどに関する研究を長期的に行なっていく計画である。
韓国	基礎研究	△	→	<ul style="list-style-type: none"> 2018 年 6 月、高麗大学は、世界第 4 位の取引量を誇る Huobi（火幣）の子会社 Huobi Korea とブロックチェーン開発の分野での産学連携に合意。Huobi Korea は、高麗大学を、韓国国内でのブロックチェーン技術の研究と技術教育の提携を拡大するための基盤とみなしている。
	応用研究・開発	△	→	<ul style="list-style-type: none"> ソウル市は、今後 5 年間で、ブロックチェーンエコシステムを創ることで、ブロックチェーンハブを目指すと言明。2021 年までに 603 億ウォン（約 60.3 億円）を投じ、200 以上のブロックチェーン企業が入居できるビジネス施設を建設するとともに、トレーニングセンターを運営して 700 名超の専門家を育成することを計画。 サムスン SDS は、2018 年 6 月に、ブロックチェーンを基盤にした金融プラットフォーム Nexfinance を発表。同社は、Nexfinance を通じ、デジタル金融ビジネスを立ち上げることを計画。 サムスン SDS は、ブロックチェーンを活用した銀行向けの個人認証ツール BankSign を開発し、2018 年 8 月に発表。全銀行間で個人認証を一括で行える技術革新を目指している。 サムスン SDS は、自社のブロックチェーン・プラットフォーム Nexledger を輸出税関ロジスティクス・サービスに活用することに、2018 年 9 月、韓国税関と合意したと発表。

(8) 参考文献

- 1) Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", <https://bitcoin.org/bitcoin.pdf> (accessed 2019-1-20)
- 2) <https://www.nature.com/articles/s41893-018-0152-7>
- 3) David Chaum, "Blind Signatures for Untraceable Payments", *Advances in Cryptology: Proceedings of Crypto 82* (Santa Barbara, California, August 23-25, 1982) pp 199-203.
- 4) Aram Mine, "ブロックチェーン上で契約をプログラム化する仕組み「スマートコントラクト」", <http://gaiax-blockchain.com/smart-contract> (accessed 2019-1-20)
- 5) Arvind Narayanan, Joseph Bonneau, and Edward Felten, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, (Princeton Univ. Pr., 2016); 長尾高弘 (訳), 『仮想通貨の教科書』(日経 BP 社, 2016).
- 6) 山際貴子, "スマートコントラクトとは? ブロックチェーン活用の仕組みと KDDI の実証実験を紹介", *ボクシルマガジン・ビヨンド* (2018.01.10) <https://boxil.jp/beyond/a3594/> (accessed 2019-1-20)
- 7) Hayata, "DAG 通貨の種類とそれぞれの特徴について", *Crypto Times* (2018-03-02) https://crypto-times.jp/explain_dag/ (accessed 2019-1-20)
- 8) おくなも, "DAG 型暗号通貨のすすめ ブロックチェーンを代替しうる新技術", BTC

- News (2017.09.22) <https://btcnews.jp/2x5fpwlo12702/> (accessed 2019-1-20)
- 9) Serguei Popov, “The Tangle” , IOTA Whitepaper Ver. 1.4.3 (update: April 29, 2018), <https://forum.helloiota.com/732/The-Tangle-whitepaper>; IOTA Fan Site (訳), https://iotafan.jp/wp-content/uploads/2018/06/iota1_4_3jp.pdf (accessed 2019-1-20)
 - 10) 日本銀行, 欧州中央銀行, 共同調査プロジェクト (Project Stella) 報告書「日本銀行・欧州中央銀行による分散型台帳技術に関する共同調査 — 分散型台帳技術による資金決済システムの流動性節約機能の実現 —」 https://www.boj.or.jp/announcements/release_2017/data/rel170906a3.pdf (accessed 2019-1-20)
 - 11) 内閣府, 戦略的イノベーション創造プログラム (SIP) 「AI (人工知能) ホスピタルによる高度診断・治療システム」 研究開発計画 (平成 30 年 7 月 19 日) http://www8.cao.go.jp/cstp/gaiyo/sip/keikaku2/10_aihospital.pdf (accessed 2019-1-20)
 - 12) e-Estonia guide, <https://e-estonia.com/wp-content/uploads/eestonia-guide-2018.pdf> (accessed 2019-1-20)
 - 13) e-Estonia FAQ, <https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf> (accessed 2019-1-20)
 - 14) Ahto Buldas, Andres Kroonmaa, and Risto Laanoja, “Keyless Signatures’ Infrastructure: How to Build Global Distributed Hash-Trees” , Proceeding of 18th Nordic Conference on Secure IT Systems (NordSec 2013; Ilulissat, Greenland, October 18-21, 2013) Vol. 8208, pp. 313-320.
 - 15) E-estonia, “Estonian Healthcare: e-Health record and e-Prescription took over,” Youtube (July 10, 2013), <https://www.youtube.com/watch?v=2XOqsJh4Abg> (accessed 2019-1-20)
 - 16) E-estonia, “E-health – Estonian Digital Solutions for Europe,” <https://e-estonia.com/e-health-estonian-digital-solutions-for-europe/> (accessed 2019-1-20)
 - 17) EU Blockchain Observatory and Forum An Initiative of the European Commission, <https://www.eublockchainforum.eu/> (accessed 2019-1-20)
 - 18) 経済産業省、「ブロックチェーン技術を利用したサービスに関する国内外動向調査」 報告書 (2016 年 4 月 28 日) <http://www.meti.go.jp/press/2016/04/20160428003/20160428003.html> (accessed 2019-1-20)
 - 19) Kentaroh Toyoda, Panagiotis Takis Mathiopoulos, Iwao Sasase, and Tomoaki Ohtsuki, “A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in The Post Supply Chain” , IEEE Access, Vol. 5, (2017) pp. 17465-17477. DOI: 10.1109/ACCESS.2017.2720760
 - 20) Shin Morishima and Hiroki Matsutani, "Acceleration of Anomaly Detection in Blockchain Using In-GPU Cache", Proceedings of the 16th IEEE International Symposium on Parallel and Distributed Processing with Applications (ISPA 2018; Melbourne, Australia, December 11-13, 2018) in press.