

研究開発の強化・ NTT Research,

先端基礎研究

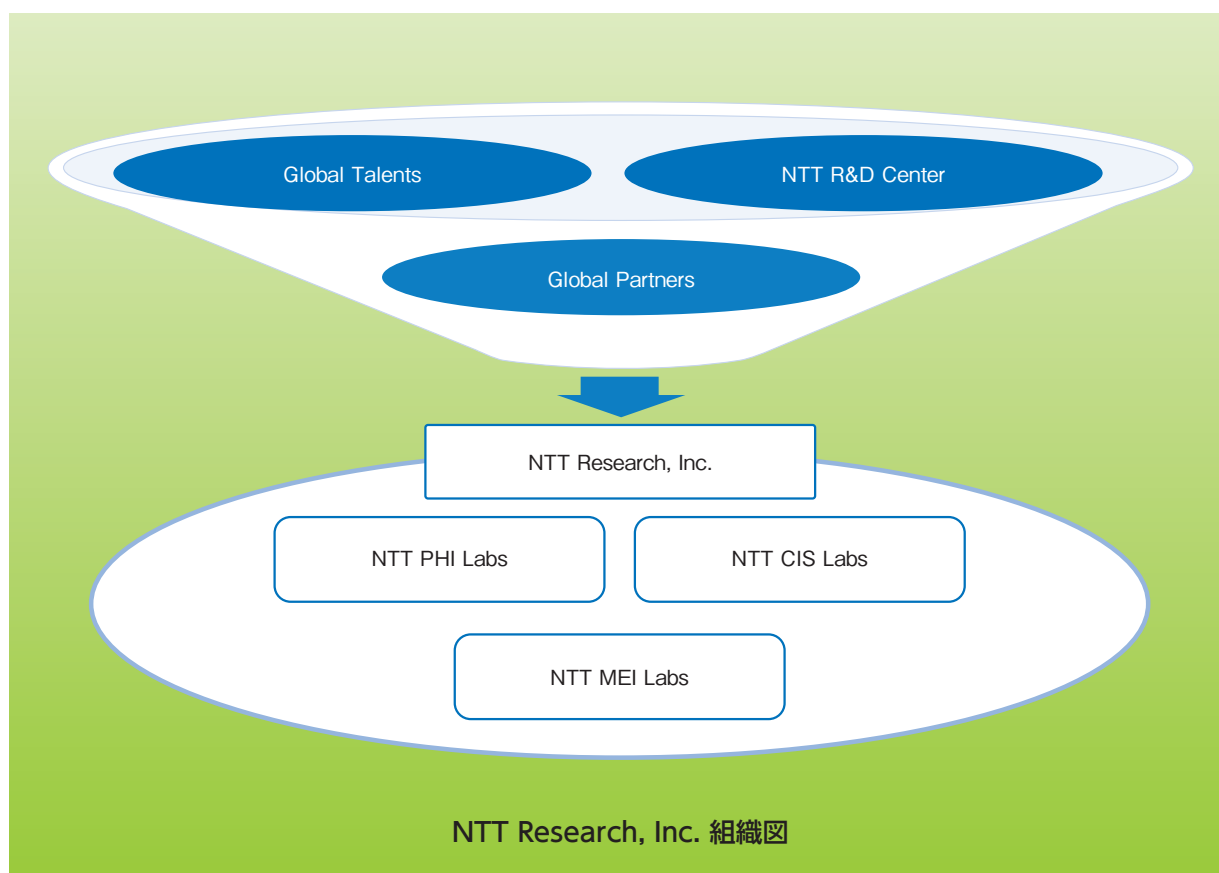
IOWN構想

量子ニューラルネットワーク

暗号

データサイエンス

2018年11月のNTTグループ中期経営戦略「Your Value Partner 2025」において発表したNTT Research, Inc. は、5～10年後の事業創造をめざして、全く新しい技術のタネをつくる基礎研究を行う。最初に取り組む「量子物理科学」「情報数学理論」「医療健康情報」の3分野において、革新的な技術を生み出すことを目標とする。本特集では各研究所の取り組みを紹介する。



グローバル化に向けた Inc. 始動

■ 研究開発の強化・グローバル化に向けたNTT Research, Inc. 始動

「量子物理科学」「情報数学理論」「医療健康情報」を主な研究領域とするNTT Research, Inc. の3つの研究所の概要、および今後の展開について紹介する。

10

■ Physics & Informatics Laboratoriesの取り組み

Physics & Informatics Laboratories (NTT PHI Labs) の研究領域を構成する概念、および室温で量子効果を実現できる光パラメトリック発振器について紹介する。

12

■ Cryptography & Information Security Laboratoriesの 目標と研究

Cryptography & Information Security Laboratories (NTT CIS Labs) の取り組みや目標、および暗号基礎理論とブロックチェーン理論を研究するそれぞれのグループについて紹介する。

19

■ Medical & Health Informatics Laboratoriesの発足

Medical & Health Informatics Laboratories (NTT MEI Labs) の取り組み、および生体情報をめぐる社会の変化について紹介する。

23

■ 2019年の暗号研究所開設にあたって

画期的な研究を生み出す企業研究所を持つことの利点について、Brent Watersの考えを紹介する。

27

研究開発の強化・グローバル化に向けた NTT Research, Inc. 始動

2018年11月のNTTグループ中期経営戦略「Your Value Partner 2025」において発表したNTT Research, Inc. は、5～10年後の事業創造をめざして、全く新しい技術のタネをつくる基礎研究を行います。最初に取り組む「量子物理学」「情報数学理論」「医療健康情報」の3分野は2019年5月に発表したIOWN（アイオン：Innovative Optical and Wireless Network）構想における新規性の根幹を支えます。NTT Research, Inc. のUpgrade Realityにご期待ください。

こ み かずひろ^{†1} からさわ けい^{†2}

五味 和洋 / 唐澤 圭

NTT Research, Inc. 代表取締役社長^{†1}
NTT Research, Inc.^{†2}

NTTのグローバル事業

NTTはグループ中期経営戦略「Your Value Partner 2025」において、成長の柱の1つとして、グローバル事業の競争力強化を進めています（図）。その中で、競争力の源泉として、イノベーションを起こすために次の3つの新会社を設立しています。1番目の創造的革新組織（NTT Disruption）は、1～3年程度の短期での事業化をめざし、お客さまと技術の価値を確認するPoC（Proof of Concept）等を通じて、

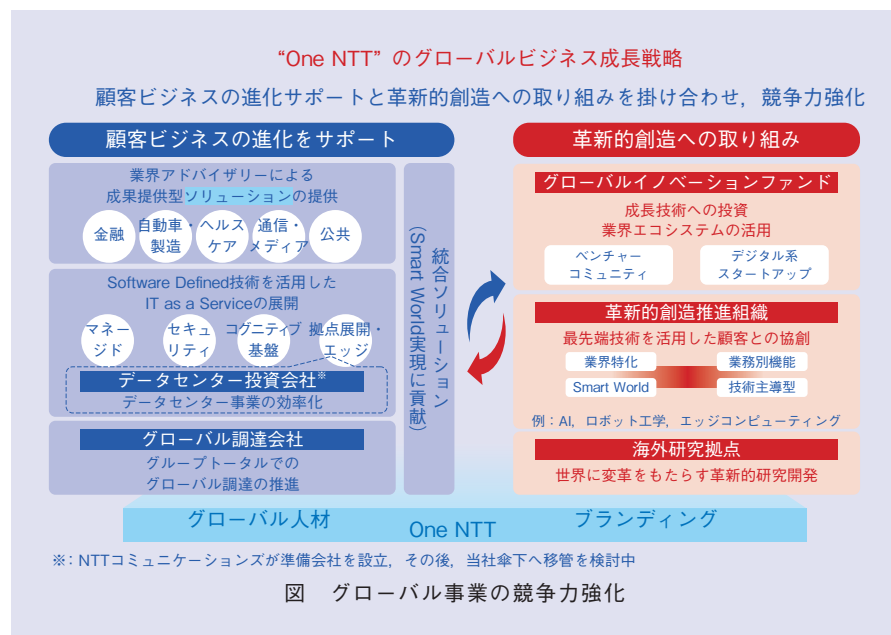
新しい技術の商用化を行います。2番目のNTT Venture Capitalは、3～5年程度の中期での事業化をめざして、ベンチャーへの投資により新しい技術の実用化を行います。3番目が、私たちNTT Research, Inc. で、5～10年後の事業創造を目標に、全く新しい技術のタネをつくる基礎研究を行います。これら3つの新会社が、NTTグループの既存の事業会社および研究所と組み合わせることで、新しい技術をグローバルに展開したいと考えています。また、3つの新会社は、シリコン

バレーに本社があります。これは、人と資金と情報が集まる場所に拠点を設けることにより、お客さまやパートナーと新しい技術を展開するスピードを速めたいと考えるからです。また、基礎的な研究活動そのものにおいて、さまざまな人と情報が集まる場所は、優れた研究者に刺激的な環境を提供できるということも、本社をシリコンバレーに置いた大きな理由です。

NTT Research, Inc. の研究領域

NTT Research, Inc. の研究領域は、国内のNTT研究所と密に連携しながら、方向性を定めています。NTT研究所では、これまでも光通信デバイスや人間心理などICTにかかわる幅広い研究分野において、基礎から応用までの長期にわたる研究プロセスを一貫してサポートすることにより、IEEEマイルストーンに選ばれるようなエポックメイキングな成果をいくつも生み出してきました。

NTTは、2019年5月にIOWN（アイオン：Innovative Optical and Wireless Network）構想を発表し、従来のコミュニケーションサービスの垣根を超えて、人間の生活をさらに豊かにする技術開発を進めています。NTT



Research, Inc.は、この構想の新規性の根幹となる光をベースとする「量子物理学」、個人情報を含むさまざまなデータの安全な活用を促す「情報数理学理論」、人間の基本データである「医療健康情報」を主な研究領域とする3つの研究所からスタートします。

- ① 量子計算科学研究所：Physics & Informatics Laboratories (NTT PHI Labs)
- ② 暗号情報理論研究所：Cryptography & Information Security Laboratories (NTT CIS Labs)
- ③ 生体情報処理研究所：Medical & Health Informatics Laboratories (NTT MEI Labs)

これらは、NTT R&Dが日本で長年培ってきた基礎技術分野であり、ここに海外の英知を掛け合わせて、さらに新たな技術の方向性をつくり出すことを目標にしています。

NTT PHI Labsでは、物理学と情報学の共創領域を探索し、基礎物理学研究、特に量子-古典クロスオーバーの物理とニューラルネットワークにおける臨界現象の接点に注目しています。また、その情報処理への応用など全く新しい理論を構築する基礎研究を推進していきます。その所長には、国立情報学研究所/スタンフォード大学の名誉教授で、内閣府の革新的研究開発推進プログラムのプログラム・マネージャーを務めた山本喜久が指揮をとります。

NTT CIS Labsでは、安心・安全な未来を構築するための暗号理論および情報セキュリティの基礎研究として、

高度先端機能に対応した暗号理論やブロックチェーン等の分散環境下における安全性理論などを探求します。その所長には、世界最先端の暗号理論研究者でありNTT フェローでもある岡本龍明が指揮をとります。

NTT MEI Labsでは、プレシジョン・メディシン（精密医療）につながる情報処理技術、特に、生体の電気現象だけでなく、診療録の情報やゲノムの情報を含む多次元で大量の生体情報を扱うdata-driven medicine技術に取り組みます。その所長には、世界のトップクラスとの交流実績を持つ榊原記念病院顧問の友池仁暢が就任しました。

NTT Research, Inc. は、これらの研究所長が持つ人脈をはじめとしたネットワークを活用して、NTT研究所が蓄積してきた独自技術を支える研究領域に、海外を含む外部の優れた研究者を招へいし、国内と連携する新たな研究チームを組成してきています。NTT Research, Inc. が実施する基礎研究のめざす独自の未来像をお客さまやパートナーに紹介することは、NTTグループが有する長期的なビジョンや、類まれな人的リソースの奥行きなど、独自の企業アセットを示すことができ、長期的なビジネスパートナーとしての価値をアピールできると考えています。NTT Research, Inc. の存在やその活動が、NTTグループ事業の発展にこのようなかたちで寄与できればと考えています。

今後の展開

本特集では、各研究所のねらいを所長から説明します。また、暗号基礎理

論の分野で特別研究員のBrent Watersが新しい研究所をつくるにあたっての思いを説明します。

NTTの研究所は、これまでもさまざまな成果をあげていますが、世界的にみるとIBMやSamsungなどの研究所が、特許数や論文数でより多くの成果をあげています。さらに、GAFA (Google, Amazon, Facebook, Apple) などの巨大企業が大学の研究室を買い取って研究活動を強化しています。私たちは、日本のNTT研究所と連携しながら、これまで築いてきた世界中の大学等の先端研究ネットワークをさらに拡大し、基礎研究の段階からより大きなエコシステムを、シリコンバレーを起点にグローバルに構築していきたいと考えています。



(左から) 五味 和洋/ 唐澤 圭

シリコンバレーの地で、Xerox PARCなどが創造してきたデジタル社会をベースに、現実世界 (Real) にさらに大きな変革 (Upgrade) を生み出したいと考えています。NTT Research, Inc. のUpgrade Realityにご期待ください。

◆問い合わせ先

NTT Research, Inc.
Corporate Strategy Office
E-mail info@ntt-research.com

Physics & Informatics Laboratoriesの取り組み

Physics & Informatics Laboratories (NTT PHI Labs) は、量子と脳の境界領域に将来の情報処理技術に変革をもたらす新原理が存在すると考え、ここに研究領域を設定しました。特に、量子—古典クロスオーバーの物理とニューラルネットワークにおける臨界現象に着目しています。この量子と脳の境界領域で動作するコンピュータをシンプルにエレガントにそして実用的に実装する手段として、光技術、特に室温で量子効果を実現できる光パラメトリック発振器にフォーカスします。本稿では、NTT PHI Labsの研究領域を構成する概念、技術、応用先について紹介します。

やまもと よしひさ

山本 喜久

NTT Research, Inc. NTT PHI Labs 所長

光パラメトリック発振器を用いた量子ニューラルネットワーク

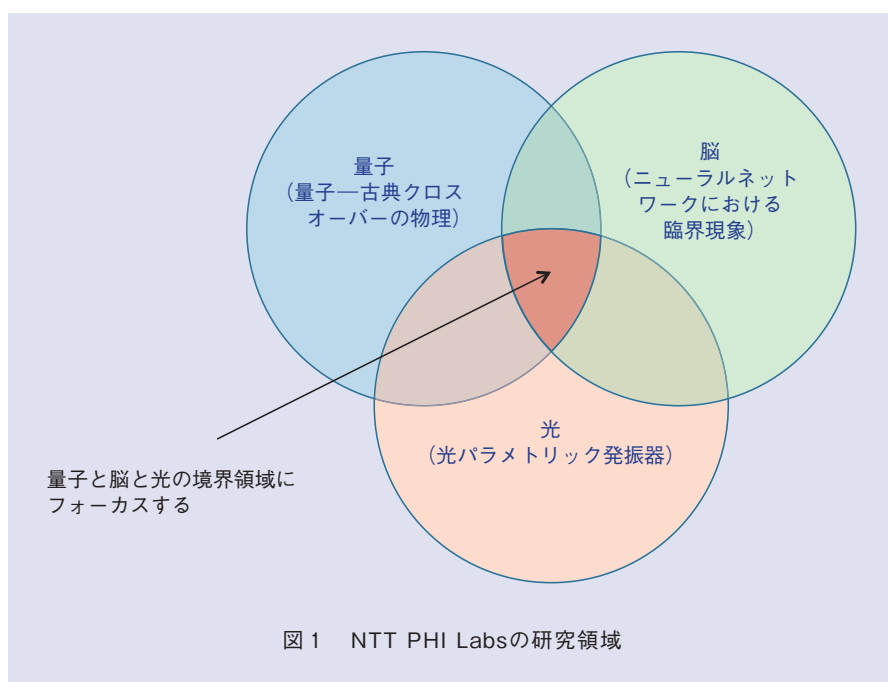
コヒーレントな電磁波を発生する発振器の開発とその応用分野の開拓は、2つの異なる原理に基づく発振器の競合の歴史でもあります。2つの発振器とは、電気工学の言葉を使えば、ポンプ源のコヒーレンスを必要としない負性抵抗発振器と、コヒーレントなポンプ波を必要とする非線形リアクタンス発振器のことを指します。どの周波数帯の発振器の開発も、まず実現しやすい負性抵抗発振器が登場し、その後より雑音の少ない非線形リアクタンス発振器が開発されるという歴史をたどってきました。紫外から赤外に至る広い波長域をカバーする光の発振器の開発の歴史もまた例外ではありません。光の負性抵抗発振器であるレーザーは、ヒューズ研究所のTheodore Maimanの手により1960年に実現されました⁽¹⁾。一方、光の非線形リアクタンス発振器である光パラメトリック発振器（特に実用上重要な連続波を発生するもの）は、スタンフォード大学のStephen HarrisとRobert Byerにより1968年に実現されました⁽²⁾。

20世紀に花開いた光通信技術は

レーザーにより支えられてきましたが、21世紀の光情報処理技術は光パラメトリック発振器により支えられるであろう、というのが私たちの将来ビジョンです。光パラメトリック発振器は、発振しきい値以下のポンプ領域では量子性の強いアナログ素子として振舞い、発振しきい値以上のポンプ領域では、古典性の強いデジタル素子として振舞います。後述するように、将来の情報処理技術は、量子計算リソースと古典計算リソースの両方を同時に必要

としますが、光パラメトリック発振器は室温でこの量子—古典の二面性を同時に実現しているほとんど唯一の素子です。

私たちは、光パラメトリック発振器をニューロンとするニューラルネットワークを構成し、これを用いて、現代コンピュータが不得意な組合せ最適化問題や量子多体問題を解こうとしています⁽³⁾ (図1)。ニューラルネットワークを構成するもう1つの要素（シナプス結合）に関しては、特にすべての



ニューロン間にシナプス結合をはる全結合型ニューラルネットワークを実現するための2つの実装方式があります(図2)。 N 個のニューロンには N 個の光パラメトリック発振器を使うのではなく、長さ1~10 kmの光ファイバリング共振器中に周回する N 個のパラメトリック発振光パルスを用います。この方法により、欠陥のない均一な N 個のニューロンが1つの共振器中に同時に実現されることになります^{(4)~(6)}。

光遅延線結合方式では、 $(N-1)$ 本の光遅延線と同数の光変調器で $N(N-1)$ 個のシナプス結合係数 $[J_{ij}]$ を実装できます⁽⁴⁾。この方式では、各時刻に、1つのターゲットパルス i に対して $(N-1)$ 個の入力パルス j が結合係数 J_{ij} を介して同時に結合されるので、 N 個のターゲットパルスすべてにこのことが実現される1周回ごとに $N(N-1)$ 個の J_{ij} が実装されることになります。また、方向性を持つ

たシナプス結合($J_{ij} \neq J_{ji}$)が簡単に実装できるメリットを有します。

一方、測定フィードバック方式では、たった1つの測定フィードバック回路で $N(N-1)$ 個の全シナプス結合を実現できます^{(5), (6)}。前者は大規模、高速、疎結合のニューラルネットワークの実装と量子多体問題への応用に適し、後者は中規模、高次非線形、密結合のニューラルネットワークの実装と組合せ最適化問題への応用に適すると考えています。

応用分野

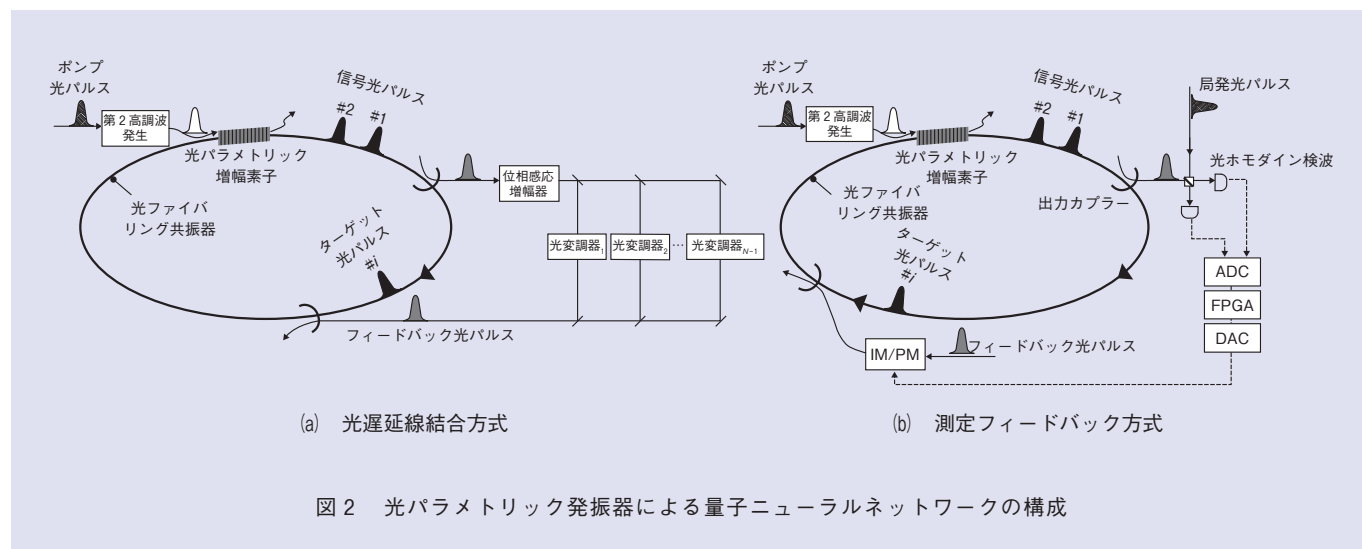
次に、この光パラメトリック発振器を用いた量子ニューラルネットワークの期待される応用分野について紹介します。

■組合せ最適化問題

組合せ最適化問題の代表格に、イジングモデルがあります。信号光とアイドラー光の周波数が等しい縮退型光パラメトリック発振器により実装されま

す⁽³⁾。最近の縮退型光パラメトリック発振器ネットワークのハードウェア技術の向上とアルゴリズムの進化によって、量子ニューラルネットワークの1つであるコヒーレントイジングマシンは大幅に高性能化し、組合せ最適化問題に特化した量子コンピュータの1つである量子アニーリングマシンや最先端アルゴリズム(BLS: Breakout Local Search)を実装したノイマン型コンピュータに対して優位性を持つまでに至っています^{(7), (8)}。さまざまな組合せ最適化問題をイジングモデルにマップして、この汎用最適化ソルバーを用いて解く時代がいずれ来ることが期待されています。具体的な問題として、創薬や生体触媒開発のためのリード最適化、無線通信ネットワークのリソース配分、圧縮センシングにおけるスパース推定、などへの応用アルゴリズム開発が行われています。

一方、連続量変数の最適化問題の代



表格としてXYモデルがあります。これを解くコヒーレントXYマシンは、信号光とアイドラー光の周波数が異なる非縮退型光パラメトリック発振器ネットワークにより実装されます⁽⁹⁾。コヒーレントXYマシンで解ける具体的な最適化問題として、ソーシャルネットワークの診断（コミュニティ検出）やFintechにおけるポートフォリオ最適化などへの応用アルゴリズム開発が行われています。

もう1つの組合せ最適化問題の代表格に、充足可能性（SAT: Satisfiability problem）問題があります。この問題を効率良く解くコヒーレントSATソルバーは、縮退型光パラメトリック発振器で再帰（リカレント）型ニューラルネットワークを構成することにより実現できます⁽¹⁰⁾。コヒーレントSATソルバーで解ける具体的な問題の1つに、ハードウェア検証とソフトウェア検証があります。

組合せ最適化問題をターゲットとするソルバーとして、パラメトリック発振器ネットワークによる計算に触発されて考案されたデジタル計算機が最近注目を集めています。光（あるいは超伝導）パラメトリック発振器ネットワークを実際に実現する代わりに、この系を記述する量子力学的運動方程式をFPGA（Field Programmable Gate Array）などのデジタル回路にアルゴリズムとしてプログラムし、一種の数値シミュレーションにより最適解を得る手法です^{(8), (11)}。

■量子多体問題

固体中の電子の振舞い、特に電子間に強い相互作用がある強相関電子系を精度良く効率的に数値シミュレーションするツールを開発することは、新材料の探索（Material Informatics）や新現象の発見（Topological Physics）に欠かせないものとなっています。特に、電子が2次元ポテンシャルに閉じ込められた2次元系には、通常の3次元系には存在しない新奇な量子現象が出現します。しかし、3次元系と異なり、2次元系では平均場近似に基づく数値シミュレーションが破綻するうえ、1次元系のような厳密解を得ることも困難です。そこで、対象とする2次元系の電子に対するハミルトニアンを制御しやすい別の量子系に人工的に実装し、この人工2次元量子系の振舞いを観測することを通して、対象である2次元電子系の物性を知ることが考えられてきました。いわゆる量子シミュレーションの概念です⁽¹²⁾。現在では、冷却原子、トラップイオン、超伝導回路などのさまざまな物理系を用いて固体中の電子物性をシミュレートする研究がさかんに行われています。

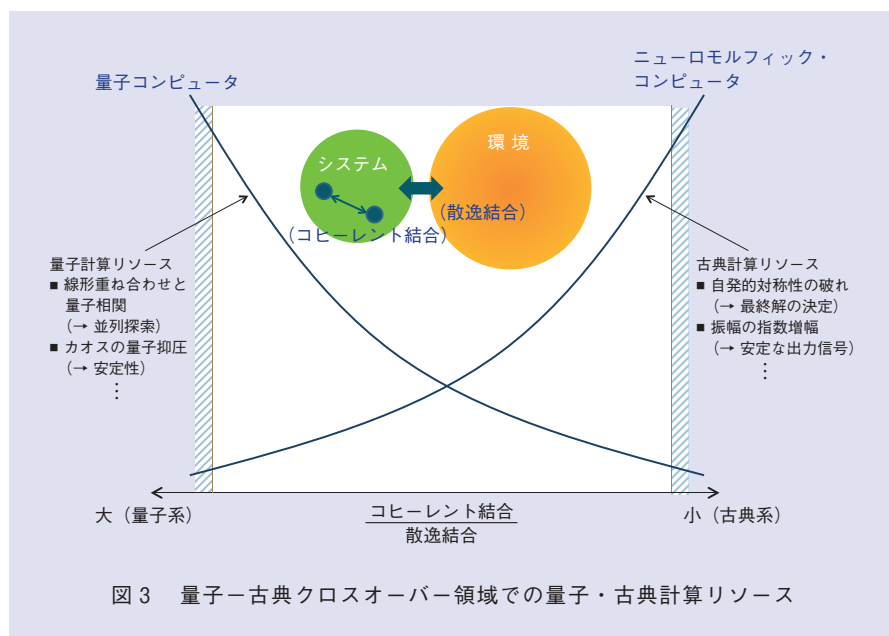
このような量子シミュレータの開発は、現在はまだ基礎研究の段階ですが、将来は、最先端デジタルコンピュータ（HPC: High Performance Computing）にさまざまな近似数値計算手法（動的あるいはクラスター平均場理論、量子モンテカルロ法、テンソルネットワーク法など）をアルゴリズムとして実装する物性物理学や量子化学の伝統的な

手法との競争にさらされることとなります。特に、シミュレーション精度、速度、装置の大きさ、価格、保守の容易さなどの多面的な要素が、将来技術としての生き残りを決定することになります。

私たちは伝統的な手法に対して競争力のある量子シミュレータの将来像として“光を使って電子をシミュレートする”装置を思い描いています⁽¹³⁾。

量子—古典クロスオーバーの物理

ミクロな世界を記述することに成功した量子論が、いつどのようにしてマクロな世界を支配する古典論に取って変わられるのか、という量子—古典クロスオーバーの問題は、量子物理学者にとってもっとも根源的なテーマです。この問題を分かりやすく理解する1つの理論モデルは、少数自由度を持つシステムが多数の（あるいは無限の）自由度を持つ環境系と結合している開放系を設定することです⁽¹⁴⁾。図3に示すように、システム内のコヒーレントな相互結合の強さに比べて、システム—環境間の散逸結合（デコヒーレンス）が小さくなるにつれて、線形重ね合わせ状態と量子相関を利用した量子並列探索や量子干渉による古典カオスの抑圧といった量子計算リソースはその有効性を増していきます。このため、量子コンピュータは、環境への散逸結合をできるだけ小さくした領域で実現されるべきものと、従来は思われてきました。量子誤り訂正コードやトポロジカル量子コンピュータといった



コンセプトは、こうした思想に沿って登場してきたものです。一方、環境への散逸結合が大きくなるにつれて、自発的対称性の破れによる最終解の非可逆的決定であるとか、選択された最終解の振幅を指数増幅して安定な古典情報として出力する、といった古典計算リソースはその有効性を増していきます。このため、人間の神経細胞の働きと仕組みを模倣する、あるいは人間の脳の思考方法から着想を得たニューロモルフィックコンピュータは、環境への散逸結合をできるだけ大きくして、システムの量子コヒーレンスを完全に除去した頑強な古典領域で実現されるべきものと、従来は思われてきました。

私たちは、量子・古典という2つの計算リソースが同時に利用できる量子-古典クロスオーバーの領域にこそ、将来のコンピュータが実現されるべき

だと考えています。光パラメトリック発振器ネットワークは、ポンプレート調整することにより、この量子-古典クロスオーバー領域を自由に行き来できるユニークなハードウェア・ソリューションです。このような考え方は、“人間の脳における高度な情報処理（意識、認知、決断といった）機能は巨大なニューラルネットワークにおける一種の相転移臨界現象に基づいている”とする最近の神経科学者の考え方（Computing at Criticality）と相通じるところがあります⁽¹⁵⁾。

なぜ、古典計算リソースも必要なのか？

組合せ最適化問題を量子コンピュータだけを使って解く方法を図4(a)に示します。まず、与えられた問題の解の (2^N) 個ある全候補を同じ確率振幅

$(1/\sqrt{2^N})$ を持つ線形重ね合わせ状態として表わし、次に、何らかの方法により最適解を同定し、この状態の振幅を $1/\sqrt{2^N}$ から1へ増幅し、他のすべての状態の振幅を $1/\sqrt{2^N}$ から0へ減衰させます。その後、 N 個の量子ビットに対して、0か1かの射影測定を行えば100%に近い確率で最適解が求められます。この手法のボトルネックは、最適解の振幅をどうやって増幅し、最適解でない他のすべての状態の振幅をどうやって減衰させるか、にあります。量子コンピュータを用いてこれを実現する最適な方法はGroverにより発見されています⁽¹⁶⁾。Grover iterationというこのルーチンを合計で $\sqrt{2^N}$ 回繰り返すと、上記終状態が得られます。このことは、量子コンピュータを使って組合せ最適化問題を解こうとすると、指数時間を費やさなければならないことを意味しています。例えば、この仮想的な量子コンピュータにはデコヒーレンスもゲートエラーも全くなく、したがって量子誤り訂正をかける必要もなく、ビット間に全結合が実装され、非局在の2ビットゲートが1nsという高速で自由に実装できると仮定し、さらに与えられた問題の最適解を何らかの方法で瞬時に同定できとします。この理想的な量子コンピュータを用いても、最適解の確率振幅を $1/\sqrt{2^N}$ から1へ増幅するためには、例えば $N = 150$ ビットという比較的小さな問題に対しても、 ~ 200 億年という長時間がかかることが示されます。同じ問題を量子ニューラルネット

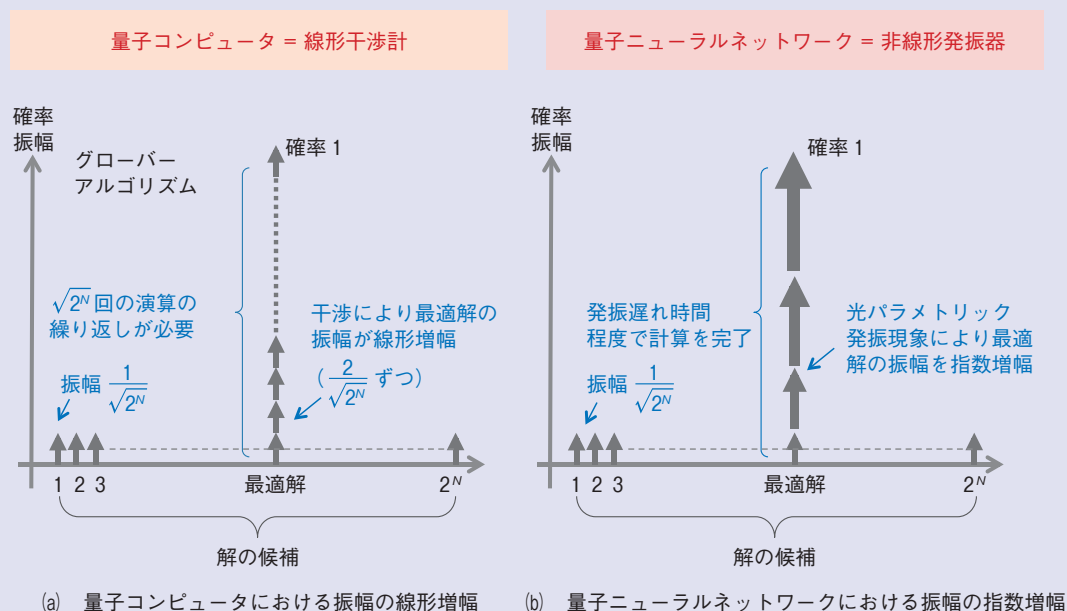


図4 組合せ最適化問題を解く2つの方法

ワークに解かせた場合の計算時間はどの程度でしょうか。図4(b)に示すように、発振しきい値以下の N 個のパラメトリック発振光パルスは0相と π 相の線形重ね合わせ状態にあるので、量子コンピュータの場合と同様、解の全候補は同じ確率振幅($1/\sqrt{2^N}$)を持つ線形重ね合わせ状態として表わすことができます。このとき、ポンプレートを発振しきい値まで上げていくと、最小のネットワーク損失を有する最適解が単一モード発振を起こし、その振幅はたかだか光子寿命($\mu\text{s}\sim\text{ms}$ のオーダー)で初期値 $1/\sqrt{2^N}$ から最終値1に指数増幅されます⁽³⁾。この指数増幅は古典系(開放系)に特有な現象で、量子系では実現できません。コピー

レントイジングマシンで組合せ最適化問題の最適解を得るのにかった計算時間(実験値)では、問題サイズ $N=150$ ビットに対して計算時間はわずか54 msでした⁽⁷⁾。

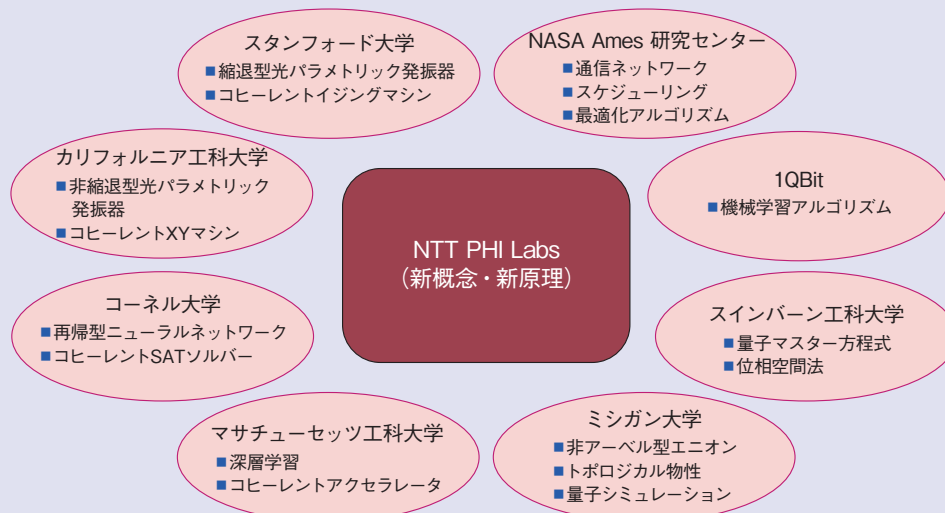
この例が示していることは、隠れた周期性を持つような特殊な問題(因数分解や離散対数など)を別として、一般的な組合せ最適化問題を高速に解くための将来のコンピュータには、線形重ね合わせ状態のような量子計算リソースだけでなく、振幅の指数増幅のような古典計算リソースも欠かせない、ということです。ただし、前述のGroverの方法は必ず特定の解を増幅することが理論的に保証されていますが、量子ニューラルネットワークでは

その理論保証はまだ確立していません(ヒューリスティック計算機)。そのため、単純な比較はできないことに注意する必要があります。

研究体制

NTT PHI Labsは量子力学を用いた情報処理に関する新概念・新原理の探索を行うことを目標に、外部研究機関との共同研究を積極的に進めていきます(図5)。

図5の体制図の左側に、主として実験グループをまとめました。スタンフォード大学チーム(Hideo Mabuchi教授, Martin Fejer教授, Benjamin Lev准教授, Surya Ganguli准教授, Amir Safavi-Naeini助教授)とは、光もし



今後、NTT R&D のソフトウェアイノベーションセンタ、物性科学基礎研究所との連携をめざす。

図5 NTT PHI Labsの外部共同研究機関とテーマ

くは超伝導パラメトリック発振器ネットワークをベースとするコヒーレントイジングマシンやニューラルネットワーク臨界現象の研究を進めています。コーネル大学チーム (Peter McMahon助教授) とは、再帰 (リカレント) 型光パラメトリック発振器ネットワークをベースとするコヒーレントSATソルバーの研究を進めています。カリフォルニア工科大学チーム (Alireza Marandi助教授) とは、非縮退型光パラメトリック発振器ネットワークをベースとするコヒーレントXYマシンの研究を進めています。マサチューセッツ工科大学チーム (Dirk Englund准教授, William Oliver教授) とは、光ホモダインミキサーをベースとするコヒーレントアクセラレータ (ディープラーニングをターゲットと

する) の研究を進めています。

図5の体制図の右側に、主として理論グループをまとめました。NASA Ames研究センターチーム (Eleanor Rieffel QAIL所長) とは、通信ネットワーク、スケジューリングなどの最適化応用アルゴリズムの研究を進めています。1QBitチーム (Pooya Ronaghグループ長) とは、機械学習向けの応用アルゴリズムの研究を進めています。スインバーン工科大学チーム (Peter Drummond教授, Margaret Reid教授) とは、位相空間法による量子確率微分方程式の研究を進めています。ミシガン大学 (Franco Nori教授) とは、非アーベル型エニオンやトポロジカル物性の光パラメトリック発振器ネットワークによる量子シミュレーションの研究を進めています。

最後に、従来の量子コンピュータと私たちが研究する量子ニューラルネットワークの違いを表に示します。

まとめ

30年以上も前のことですが、当時AT&T-NTT幹部会合なるものが両社の研究所間で毎年開催されていました。北原副社長に率いられたNTT研究所メンバの1人として、ニュージャージー州のベル研究所を訪問したときのことを思い出します。紹介されたベル研究所トップ (社長) は英国人、基礎研究担当の副社長はドイツ人、物理部門を統括するエグゼクティブディレクターはインド人でした。そして、理論物理を担当する (通称Physics 001と呼ばれていた) ディレクターは米国人でした。この方がAT&T-NTT

表 2つの量子計算モデル

物理系	量子ユニタリ計算 孤立系（量子コンピュータ）	量子散逸計算 開放系（量子ニューラルネットワーク）
原理	外界から遮断された孤立系での状態ベクトルの ユニタリ回転	外界からの励起、外界への散逸のある開放系での 自己秩序形成
提案	Deutsch(1985)：量子並列探索 Shor(1994)：量子アルゴリズム	Zurek(2003)：量子ダーウィニズム Cirac(2009)：ユニバーサル量子計算
リソース	量子エンタングルメント	量子ディスコード
長所	物理が明確 ユニバーサル計算	雑音やエラーに対して強靱
短所	雑音やエラーに対して脆弱	物理が見えにくい ヒューリスティック計算
応用分野	隠れた周期性や構造のある問題 (現代暗号の解読など)	周期性や構造のない問題 (組合せ最適化など)

幹部会合で基調講演を行ったときに基礎研究担当のArno Penzias副社長（1978年ノーベル物理学賞）が「そんなに早くしゃべったら、君はこの部屋の聴衆の半分を失うことになるぞ」と厳しく叱責したことが忘れられません。いつか、このようなNTT研究所をつくりたい、というのが私の夢になりました。私たちはスタートラインに立ったのです。

■参考文献

- (1) T. Maiman: "Stimulated Optical Radiation in Ruby," Nature, Vol.187, pp.493-494, August 1960.
- (2) R. L. Byer, M. K. Oshman, J. F. Young, and S. E. Harris: "VISIBLE CW PARAMETRIC OSCILLATOR," Appl. Phys. Lett., Vol.13, No.3, p.109 August 1968.
- (3) Z. Wang, A. Marandi, K. Wen, R. L. Byer, and Y. Yamamoto: "Coherent Ising machine based on degenerate optical parametric oscillators," Phys. Rev. A, Vol.88, No.6, 063853, Dec. 2013.
- (4) A. Marandi, Z. Wang, K. Takata, R. L. Byer, and Y. Yamamoto: "Network of time-multiplexed optical parametric oscillators as a coherent Ising machine," Nature Photonics, Vol.8, p.937, Oct. 2014.
- (5) T. Inagaki, Y. Haribara, K. Igarashi, T. Sonobe, S. Tamate, T. Honjo, A. Marandi, P. L. McMahon, T. Umeki, K. Enbutsu, O. Tadanaga, H. Takenouchi, K. Aihara, K. Kawarabayashi, K. Inoue, S. Utsunomiya, and H. Takesue: "A coherent Ising machine for 2000-node optimization problems," Science, Vol.354, No.6312, pp.603-606, Nov. 2016.
- (6) P. L. McMahon, A. Marandi, Y. Haribara, R. Hamerly, C. Langrock, S. Tamate, T. Inagaki, H. Takesue, S. Utsunomiya, K. Aihara, R. L. Byer, M. M. Fejer, H. Mabuchi, and Y. Yamamoto: "A fully programmable 100-spin coherent Ising machine with all-to-all connections," Science, Vol.354, No.6312, pp.614-617, Nov. 2016.
- (7) R. Hamerly, T. Inagaki, P. L. McMahon, D. Venturelli, A. Marandi, T. Onodera, E. Ng, C. Langrock, K. Inaba, T. Honjo, K. Enbutsu, T. Umeki, R. Kasahara, S. Utsunomiya, S. Kako, K. Kawarabayashi, R. L. Byer, M. M. Fejer, H. Mabuchi, D. Englund, E. Rieffel, H. Takesue, and Y. Yamamoto: "Experimental investigation of performance differences between coherent Ising machines and a quantum annealer," Science Advances, Vol.5, No.5, eaau0823, May 2019.
- (8) T. Leleu, Y. Yamamoto, P. L. McMahon, and K. Aihara: "Destabilization of Local Minima in Analog Spin Systems by Correction of Amplitude Heterogeneity," Phys. Rev. Lett., Vol.122, No.4, 040607, Feb. 2019.
- (9) Y. Takeda, S. Tamate, Y. Yamamoto, H. Takesue, T. Inagaki, and S. Utsunomiya: "Boltzmann sampling for an XY model using a non-degenerate optical parametric oscillator network," Quantum Sci. Technol., Vol.3, No.1, 014004, Nov. 2017.
- (10) M. Ercsey-Ravasz and Z. Toroczkai: "Optimization hardness as transient chaos in an analog approach to constraint satisfaction," Nature Physics, Vol.7, pp.966-970, Oct. 2011.
- (11) H. Goto, K. Tatsumura, and A.R.Dixon: "Combinatorial optimization by simulating adiabatic bifurcations in nonlinear Hamiltonian systems," Science Advances, Vol.5, eaav2372, April 2019.
- (12) R. P. Feynman: "Simulating physics with computers," Int. J. Theoretical Physics, Vol.21, pp.467-488, June 1982.
- (13) M. D. Fraser S. Höfling, and Y. Yamamoto: "Physics and applications of exciton-polariton lasers," Nature Materials, Vol.15, pp.1049-1052, Sept. 2016.
- (14) W. H. Zurek: "Decoherence, einselection, and the quantum origins of the classical," Rev. Mod. Phys., Vol.75, No.3, pp.715-775, July 2003.
- (15) J. Beggs: "Editorial: Can There Be a Physics of the Brain?," Phys. Rev. Lett., Vol.114, 220001, June 2015.
- (16) L. K. Grover: "A fast quantum mechanical algorithm for database search," Proc. of 28th Annual ACM Symposium on the Theory of Computing, pp.212-219, 1996.



山本 喜久

レーザのコヒーレンスを通信に応用するコヒーレント光通信の研究がNTT基礎研究所で始まったのは1979年のことでした。40年の歳月を経て、光パラメトリック発振器のコヒーレンスを情報処理へ応用する量子ニューラルネットワークの研究をスタートできるまで、光技術は進歩をとげてきました。

◆問い合わせ先

NTT Research, Inc.

NTT PHI Labs

E-mail info@ntt-research.com

Cryptography & Information Security Laboratoriesの目標と研究

2019年7月に米国シリコンバレーで発足したNTT Research, Inc. の3つの研究所の中の1つがCryptography & Information Security Laboratories (NTT CIS Labs) です。NTT CIS Labsでは、暗号分野の理論研究を行い、暗号基礎理論を研究するグループとブロックチェーン理論を研究するグループを持っています。本稿では、このような体制で出発したNTT CIS Labsが何をめざしてどのような研究を行うかについて紹介します。

おかもと たつあき†1

†2

岡本 龍明 /Brent Waters

まつ お しんいちろう†2

松尾 真一郎

NTT Research, Inc. NTT CIS Labs 所長†1
NTT Research, Inc.†2

はじめに

Cryptography & Information Security Laboratories (NTT CIS Labs) は、暗号基礎理論を研究するグループとブロックチェーン理論を研究するグループを持ち、暗号基礎理論グループの中には、Brent Waters を室長として暗号理論を深く研究するWaters研究室を設けています。本稿では、Waters研究室とブロックチェーングループについて焦点を当て、NTT CIS Labsの取り組みや目標、研究内容について紹介します。

暗号基礎理論研究グループ Waters研究室の取り組み

私たちは従来の暗号機能を超えた新たな暗号機能を実現することから、暗号基礎理論をより良くより深く理解することまでさまざまな分野の暗号理論の研究を行います。最初に注力するテーマの1つが暗号システムです。

暗号は、対処とするデータを特定の受信者だけが復号して読むことができるような暗号文に変換するプロセスです。暗号は私たちのセキュリティエコシステムの基盤です。それらは物理的に盗まれる可能性のあるデバイス

(ラップトップPC、携帯電話など) や、第三者のクラウドサーバなどに格納されているような機密情報を守るために使われています。また、暗号はしばしば大きくマスコミで取り上げられることも多く、例えば2015年のサンバーナーディーノでの乱射事件での議論や、ある事件の容疑者のiPhoneの暗号解読にApple社が強要されるべきかなどの議論がありました。

従来は利用者が公開鍵pkを公開し、それに対応する秘密鍵skを秘密に保持するという暗号の姿が広く知られていました。ある人がデータmsgを公開鍵pkを使って暗号文ctに暗号化するとします。このとき、データmsgはskを持つ者だけが復号でき、その鍵を知らない攻撃者はmsgについて一切の情報を知り得ません。

ところが最近になって、暗号に関するこのような姿は多くの応用にとってあまりに制約が大き過ぎることを認識するようになりました。例えば、アリスのメールサーバが彼女の公開鍵で暗号化されたメールを受信し、保存しているとします。このとき、彼女は保存された暗号文のうちスパムメールは自動的にサーバが削除するようにしたい(現時点では、サーバによってはそれ

を復号して削除している) とか、メールの内容に彼女の子どもの名前や「非常」「病院」などといった言葉が含まれていればサーバに警告メッセージを出してほしいといった要望を持っているとします。このような機能を実現するため、彼女は自分の秘密鍵をサーバに渡すこともできます。しかし、このことは第三者に彼女のすべてのメールを読むことを許すことになります。一方、彼女が秘密鍵を管理している以上、スパム削除や非常警告といった機能を楽しむことはできません。これは、私たちが望む機能を手に入れるために従来の暗号の概念を超えた新たな概念や方式を生み出す必要を示した典型的な例となっています。現在、暗号分野では、このことが大変重要な目的であることが広く認識されており、そのような方向に沿ってさまざまな概念の暗号がつくられるようになってきました。そのような概念として、関数型暗号、完全準同型暗号、IDベース暗号、属性ベース暗号、トレータ追跡、代理再暗号化やそれ以外にも多くの概念が提案されるようになってきました。

私たちの研究所においても、このような研究を強力に推し進めていきます。目標の1つは、標準仮定の下で安

全性が証明された高度な機能を持った暗号方式を実現することです。まずは、以下の3つの分野に焦点を当てて研究を進めていきます。

■選択暗号文安全性

選択暗号文安全性 (IND-CCA) は従来の暗号においても新たな暗号機能においてもいずれも正しい安全性概念となっています。しかし、多くの新たな暗号の結果は、選択平文 (IND-CPA) モデルでその暗号機能の安全性を論じています。最近、私たちはどのようなIND-CPA安全な属性ベース暗号 (ABE) も、hinting PRGと呼ぶ新たな手法を用いることでIND-CCA安全なABEに変換できることを示しました。そこで、数論の手法を用いてより高速でコンパクトなhinting PRGを実現することをめざします。さらに、ABEを超えてより一般的な関数型暗号や再ランダム化暗号に対しても適用できるIND-CCA変換方法の実現をめざしていきます。最後に、これはIND-CPAを証明すればIND-CCAを意味するかという古典的な問題を新たな発想で解決しようとするアプローチとなっています。

■暗号システムの追跡

トレータ追跡は、放送システムにおいて不正コピーした元デコーダ装置を追跡する問題です。私たちは最近、共謀不可な追跡システムとしてN利用者

に対して $\lg(N)$ サイズの暗号文となる方式を実現し、その安全性を標準仮定の1つであるLWE (Learning with Errors) 仮定の下で証明しました。従来の標準仮定に基づく最良の結果では、暗号文サイズが $N^{1/2}$ でした。ここで、私たちが新たに目標とする問題は次のようなものを含みます。

- ・どのような定数 c に対しても暗号文サイズが $N^{1/c}$ の追跡・放送システムの実現
- ・上記と同じ暗号文サイズで公開追跡機能の実現
- ・追跡手法を利用した適応的安全性の証明手法の開拓

■LWEに基づく暗号における新たな開拓

LWE仮定はその耐量子計算機安全性や格子のワースト問題との関連において暗号における優れた方法として広く認識されています。また、よく検証された仮定から新たな暗号機能をつくる手法としてもLWE仮定を用いた方法は多くの結果を生み出してきました。例えば最近の結果として、完全準同型暗号、任意の回路に関する属性ベース暗号、ロック可能難読化などがあります。これらは、今のところ、他の標準的な数論仮定を用いては実現されていません。ここで私たちは、LWEベース暗号を実現する新たな野心的な目標を提案します。まず最初に

疑似ランダム関数を難読化する新たな概念とその応用を検討します。次にLWE仮定から証拠暗号をつくるための方法を述べます。そこへの中間段階として、ビットを定めた機能に対する制限付きPRFを実現します。

私たちの理論研究所はこの分野で幸先の良いスタートをしました。WatersとDaniel Wichsは、共著のCrypto2019論文にて、暗号文サイズが $N^{1/c}$ の追跡・放送機能をLWEに基づくトレータ追跡と双線形写像による放送暗号の手法を組み合わせることで実現しました。現在、Waters, WichsとMark Zhandryは、LWEベースの属性ベース暗号の適応的安全性を実現する新たな手法と限界について共同研究を行っています。

ブロックチェーン理論研究グループの取り組み

■ブロックチェーンの歴史

2008年にSatoshi Nakamotoがビットコインの論文を公表して以来、暗号技術、ピー・ツー・ピー (P2P) ネットワーク、ゲーム理論、経済学などの要素を組み合わせたインターネット上における新たなデータの信頼モデルの基盤として、ブロックチェーンと呼ばれる技術が、幅広い注目を集めています。ビットコイン自体は、支払いの履歴の帳簿を、中央管理を行う主体なし

に、P2Pネットワークに接続されたユーザの協力の下で、一定時間ごとに更新していく仕組みです。そして、その帳簿に記録されたデータそのものをお金のように考えることで、ユーザ間の支払い（Payment）に応用したものです。ビットコイン自体は、支払いというアプリケーションに特化したシステムになっています。しかし、「P2Pで接続されたユーザの協力で、共通の帳簿をアップデートしていく」という仕組みは、支払い以外のアプリケーションが広く考えられるために、その中核的なプロトコルの部分を「ブロックチェーン」と名付けて、より汎用的な技術として世界中で研究開発が行われています。

ブロックチェーンの研究のインパクトを理解するための一番のキーワードは、Permissionless Innovation（許可のいらないイノベーション）です。インターネットが中央的な組織を介さないグローバルな通信を実現し、誰もが新しいイノベーションのつくり手になるチャンスをつくり出しました。ブロックチェーンは、帳簿の維持と多様なステークホルダーがプログラム可能な帳簿を共有し、帳簿に基づいた新しいアプリケーションを誰もが自由につくり出せるようにするというインパクトがあります。ブロックチェーンの有望なアプリケーションは何かという質問

は、インターネットの有望なアプリケーションは何かという質問と同じで、個別の明確な答えがあるわけではなく、むしろ誰もが新しいアプリケーションを思いついて実験できる場がある、ということそのものに価値があります。

上記の意味において、ブロックチェーンにおける研究開発の大きなゴールは、「プログラム可能な共有された帳簿を利用したアプリケーションを、誰もが自由につくり出すことができるような状態を実現する」ことです。ビットコインやブロックチェーンが近年大きく話題になり、あたかも広く普及する時期が間近であるようにも思えますが、実際に上記のゴールを達成するのは、非常に大きなチャレンジであり、長期にわたる基礎的、理論的な研究開発が必要であるのが現状です。

ブロックチェーンを構成する部品となる技術は、実は枯れた技術が多くあります。ブロックチェーンに使われる電子署名アルゴリズムECDSAや、暗号学的ハッシュ関数SHA-256は、長い歴史を持つ標準的な暗号アルゴリズムです。また、情報のハッシュ値を計算し、それをリンクさせていくことで、情報の存在の前後性を証明できるようにする暗号学的タイムスタンプも1990年の暗号技術のトップカンファレンスCRYPTOで発表されたもので

す。P2Pの通信を使って、帳簿のデータをすべての参加者で共有する技術も新しいものではありません。また、分散コンピューティングの世界では、複数の計算機の間でのデータの内容を合意する合意プロトコルの研究も長い歴史があります。ビットコインにおいては、セキュアな合意プロトコルとしてProof of Workと呼ばれるプロトコルが採用されていますが、これも元々はスパムメールを減らす方法の一環として暗号学的パズルと呼ばれる技術の1つの例として発明され、ハッシュベースの電子マネー方式であるHashCashの中で確立されていたものです。しかし、ビットコインとブロックチェーンが画期的であったのは、それらの枯れた技術を絶妙に組み合わせ、それまでには存在していなかった、中央サーバがなくても、一定のビジネスルール（例えば支払い）に従ったプログラムで帳簿をアップデートできる方法を初めて提示したことにあります。また、こういったネットワークが持続的に存在するために、ネットワークの維持に協力した人に新しいビットコインなどの暗号資産を付与するという、インセンティブ構造をシステムに組み込んだことが挙げられます。

■ブロックチェーンの課題

ブロックチェーンのセキュリティは、単に暗号学やネットワーク理論だ

けに支えられているわけではなく、前述のようなインセンティブ設計の妙が大きく寄与しています。また、性能とセキュリティの間には複雑なトレードオフの関係が存在しており、単純に性能を向上させようとする、セキュリティが犠牲になるという微妙なバランスの上に成り立っています。現時点では、どのようなトレードオフの関係にあるのか、という点も理論的に十分解明されているわけではありません。むしろ、これからその理論的關係を明らかにして、より多くのユーザが、十分な性能を持ってブロックチェーンを使えるようにするための理論構築と実証を改めて1から行う必要があります。これは、極めて基礎的で長期的な研究課題であるといえます。ブロックチェーンにおける、理論的な大きな問題として知られているのは、スケーラビリティ問題で、オリジナルのビットコインでは1秒当たり7トランザクションしか全世界で処理することができませんが、ビットコインのセキュリティの良さを損なうことなく、処理性能を上げるということは理論的に困難な問題で、世界中でこの問題を解決するための基礎的な研究が行われています。

■異なる専門性を持った研究者で構成

NTT CIS Labsのブロックチェーングループでは、前述のブロックチェー

ンの根本的な大きなゴールを実現するための基盤的な研究にフォーカスを当てています。特にフォーカスを当てるべき研究領域として、セキュアかつよりスケーラブルな分散合意アルゴリズムの研究、プログラム可能な帳簿のための安全なプログラミング環境を実現するための研究、そして、ブロックチェーン上での情報処理を行う際のプライバシー保護の実現のための研究に取り組んでいます。

前述のとおり、ブロックチェーンの理論研究はさまざまな異なる性質が絶妙に組み合わせられているため、異なる専門性を持った研究者のチームを組む必要があります。そのため、ブロックチェーングループのメンバーも、必要な専門性を考慮して構成しています。暗号プロトコルの安全性の専門家、ソフトウェアエンジニアリングの専門家、形式検証の専門家、そしてゲーム理論と経済学の専門家など、それぞれの分野で、第一線の研究者がグループに加わっています。ブロックチェーンはまだ若い研究分野であることもあり、今後トップレベルの研究成果を出すことが期待されるポストドクターや助教年代の研究者を早いうちに集めることも重要であり、そのような研究者も加えていく方針です。さらに、FacebookのLibraに対する各国規制当局の反応にも表れているように、規制

当局の方針との整合性も、研究を進めていく時点ではバイデザインで考慮する必要があります。ブロックチェーンにまつわる規制の研究で先進的な米国の大学との共同研究も予定しています。



(左から) 岡本 龍明/ Brent Waters/
松尾 真一郎

新たに米国シリコンバレーに誕生したNTT CIS Labsが何をめざしてどのような研究を行うかについて紹介しました。新天地で世界トップの研究者を集めてスタートした研究所から、暗号基礎・ブロックチェーン理論分野で世界をリードする結果が数多く生まれることを期待してください。

◆問い合わせ先

NTT Research, Inc.
NTT CIS Labs
E-mail info@ntt-research.com

Medical & Health Informatics Laboratoriesの発足

NTT Research, Inc.に医療や健康（ヘルスケア）の分野における情報技術の基礎研究拠点としてMedical & Health Informatics Laboratories（NTT MEI Labs：生体情報処理研究所）が発足しました。本稿では、生体情報をめぐる社会の変化と新しい研究所の取り組みについて紹介します。

ともいけ ひとのぶ

友池 仁暢

NTT Research, Inc. NTT MEI Labs 所長

生体情報研究の歴史

2018年11月28日、次世代技術の基礎研究を担う3つの海外新研究所の設立がNTTから報道発表されました。医療分野については、「プレジジョン・メディシン（精密医療）につながるAIなど生体情報の分析技術に取り組みます」と方針が示されました。半年余の準備を経て2019年7月1日にMedical & Health Informatics Laboratories（NTT MEI Labs）が発足しました。

生体情報の研究の歴史は1962年日本ME（Medical Electronics and Biological Engineering）学会創立にさかのぼります。近年になって、生体情報の範囲は医療でのICT（Information and Communication Technology）の活用が進むにつれてより広がってきました。その変化の速さは、Translational Medicineという分野の名称が、数年を経ずしてTranslational Bioinformaticsと変更になったことから伺えます⁽¹⁾。AMIA（American Medical Informatics Association）のTranslational Bioinformaticsが何を包含する分野なのかという説明はいまや古典に属するものかもしれません

が、「... the development of storage, analytic, and interpretive methods to optimize the transformation of increasingly voluminous biomedical data into proactive, predictive, preventative, and participatory health. Translational bioinformatics includes research on the development of novel techniques for the integration of biological and clinical data and the evolution of clinical informatics methodology to encompass biological observations.」とあります。研究分野を広くとらえ、かつ研究が何をめざすのか（研究の出口）についても明確にしています。NTTが提唱するSmart Worldに近い概念といえるでしょう⁽²⁾。したがって、NTT MEI Labsが取り組む生体情報の範囲は、バイオロジカルな現象だけでなく、診療録の情報、ゲノムの情報、情報処理技術も含まれることになります。

医療の研究は、実験室医学研究、臨床研究（非侵襲・侵襲、観察・介入）、疫学研究に大別されます。生体情報やデータサイエンスはこれらの3領域の対象あるいは解析手段として重要な位置を占めます。このように各研究分野

を横断する情報技術を基礎研究対象とした研究所の構想は、NTT MEI Labsのほかに例をみないでしょう。

医療と健康における情報の特徴

診断、治療、予防は診療録に記録として残されています。日本は、国民皆保険が達成されていますので、診療録は医療保健行政の公的記録だともいえます。これらの情報を研究開発に利用することは目的外使用になりますので禁じられてきました。また、臨床研究における情報の収集とその利活用は、患者への十分な説明とその結果としての文書同意が研究実施の前提となります。そのうえで、集められた情報が適正に管理されているという実務と実体を伴うことが研究遂行の条件になります。スマートフォンやさまざまな携帯デバイスのアプリは健康のモニタ情報を提供していますが、それらを収集し、データとして利活用することは、個人情報保護の規定から、臨床研究と同様の手続きが求められています。NTT MEI Labsが海外で臨床の基礎的研究を行う場合は、それぞれの国における個人情報保護法を遵守することになります。米国においてはHIPAA（Health Insurance Portability and Account-

ability Act), 欧州においては2018年5月25日から改正施行されている「一般データ保護規則 (GDPR: General Data Protection Regulation)」の条件を満たさねばなりません。

近年、医療とヘルスケアの領域でもイノベーションが強調されています。産業やビジネスの世界で重要視されている特許や知財についての考え方もこの領域に強く浸透しつつあります。デバイスの開発や生体機能の新規発見等は知財として周知の手続きが必要になっています。したがって、NTT MEI Labsの基礎研究についても規範や規制についての幅広い理解が研究の企画・運営に必要な条件となります。

臨床におけるデータの利活用に関する国内の動きをみると、個人情報保護の理念が、時間をかけて一步一步、さまざまな方向で確立されてきた経緯を伺うことができます。診療情報・健康情報の電子化のあるべき姿については、2001年厚生労働省が公表した「保健医療分野の情報化に向けてのグランドデザイン」が嚆矢となりました⁽³⁾。「個人情報の保護に関する法律」は2005年に全面施行され⁽⁴⁾、2015年に改正されました。2018年5月には匿名化によるデータの共有などの「医療分野の研究開発に資するための匿名加工医療情報に関する法律（次世代医療基

盤法）」が施行されるに至っています⁽⁵⁾。このように、診療データの個人情報保護の受け止め方が多くのコンセンサス、試験的取り組み、法令成立と時間をかけた検討と整備が重畳化して進んできています。

近年、地域医療連携やEHR (Electronic Health Record) における医療情報が異なる医療機関の間で随時に相互に参照することも求められるようになりました。国は、「健康・医療戦略推進法（平成26年法律第48号）」を制定し、医療・介護・健康分野のデジタル基盤の構築を進めています⁽⁶⁾。

このように、生体情報の基礎研究は社会の倫理 (Ethical)、法律 (Legal) や規範 (Social Implication) と密接なかかわりを持ちながら進む領域であることが分かります。このとらえ方はELSIと略称されています⁽⁷⁾。また、その到達点はより良い健康や医療でありますので、社会実装の視点・工夫も欠かせぬ重要な点だと思われます。

データが期待される時代

産業や社会がめざすべき未来社会の姿あるいは技術的なコンセプトとしてIoT (Internet of Things), Society 5.0, Industry 4.0が提唱されるようになりました。その基本はデジタルデータに基づいた生産性を高めるための取

り組みですが、その特徴は情報技術が新しい知識やエビデンスをつかみ出し変革につなげていくという循環による持続的発展の仕組みではないかと思われます。この概念は医療の改革に大きな影響を与えています。例えば、診察時に発生するデータを自動収集し、ICTを駆使してこれらのデータから新たな医学知識を抽出し、その知識を活用してさらに良い診療を実現するというデータ・ドリブン (data-driven) の循環のシステムです。2007年、IOM (Institute of Medicine, 現 National Academy of Medicine) は、Learning Health Systemを提案しています⁽⁸⁾。

このように医学医療の分野でデータの集積とICTの重要性が年々高まってきました。AI (人工知能) による画像診断やヒトゲノムの臨床応用などは時代を画する大きな成果だと思われます。このようなことから、ビッグデータやICTをめぐる世界的な競争が始まっています。その緊迫感は、2018年6月米国のNIHの戦略計画, “Strategic Plan for Data Science” に示され、具体的な計画が国レベルで策定されています⁽⁹⁾。その冒頭の文章に、「As articulated in the National Institutes of Health (NIH)-Wide Strategic Plan and the Department

of Health and Human Services (HHS) Strategic Plan, our nation and the world stand at a unique moment of opportunity in biomedical research, and data science is an integral contributor.」と記されています。この宣言の根底には2015年大統領の年頭教書で目標として掲げられたprecision medicine initiativeがあると思われまふ。Precision Medicineは“がんの領域”から広く医療全般に浸透しつつあります。ここでもデータサイエンスは新しい概念の産婆役として実現の要になります。

ICT化の社会環境の変化に呼応するように世界の情報量は指数関数的に増加しています。その量は2017年から2020年にかけて約1.9倍に増加し、2020年には1カ月当り228エクサバイトに達すると予測されています⁽¹⁰⁾。IoTデバイス数の伸びが見込まれる領域の1つに医療が挙げられています(2014年と2020年の対比で3倍)。医療分野では、ゲノム情報や医療画像等あらゆる情報がデジタル化されてきており、医療IoTの急速な拡大とともにそれらの情報量の増大は今後さらに加速されると予測されます。大きな医療機関では画像診断のためにモダリティごとに大きなサーバが立てられていますが、サイロ化現象やメモリ枯渇化が

憂慮されています。このような情報爆発への処方箋としてNTTが取り組む「IOWN (Innovative Optical and Wireless Network)」の医療分野への技術展開が期待されます⁽²⁾。情報をどのように分析し総括・活用するのが、NTT MEI Labsの永続的な課題であると考えられます。

医療におけるデータサイエンスの条件

データとして入力される用語が文字上で同じであってもその定義が専門分野や地域で異なれば、あるいは生体信号が異なるキャリブレーションや特性の異なるデータ処理を経たものと一緒に取り扱われると、集積したデータから新しく知識を獲得することは不可能に近いと思われます。したがって、医療分野こそ、データの標準化はデータサイエンスを成立させるために重要な要素となります。よく知られているものに、画像の標準形式としてDICOM[®] (Digital Imaging and Communications in Medicine)、用語類の標準規格にSNOMED-CT (Systematized Nomenclature of Medicine Clinical Terms) があります。日本で進められているDPC (Diagnosis Procedure Combination) は、診断病名の標準化をICD10に準拠することで果たしていま

す。NDB (National Database) のレセプト情報、特定健診等の情報はビッグデータとして整備されており、その研究に期待が寄せられています。

医療でのICTは、電子診療録やPHR (Personal Health Record) の運用、あるいは連携診療支援に活用されてきましたが、AIやビッグデータの出現で、その役割は今後ますます大きくなると考えられます。ここでも、ICTの標準化が先行して行われなければなりません。診療におけるICTを急速に全国展開できた米国では、法整備(HITEC)と連邦事業体(ONC)が大きな役割を果たしています。

前述した米国の戦略計画では、医学研究のデータは、Findable, Accessible, Interoperable, Reusableであるべきだとしています⁽⁹⁾。データの活用と共有におけるこのFAIR principleは、医療やヘルスケアのデータを扱うときに個人情報保護や守秘義務を尊重しながら行う研究が拠って立つべきデータへの基本的な姿勢と考えられます。

NTT MEI Labsの取り組み

医療の研究は、EBM (Evidence-Based Medicine) から多次元の大量のデータを扱うdata-driven medicineに向けて動き出しています⁽¹¹⁾。NTT

MEI Labsは、従来の研究分野を横断する“対象”と“情報技術”をテーマにしていますので、医療と健康に貢献できる知見や提案を生み出し、科学的にもインパクトの高い研究が期待されます。研究の質を決めるのは、問題設定の正鵠性、データの質（正確さ、精度、量）、データ集積と分析の速さが肝だといわれています。ここでもSmart WorldとNatural Technologyをめざす「IOWN」が道しるべになるでしょう⁽²⁾。医療研究の特徴は、フィールドにおける臨床研究と基礎研究の相互移行性です。基礎研究のテーマや仮説は、臨床現場での観察や研究が端緒となった事例も少なくありません。また、NTT MEI Labsは精度の高いデータをデータバンクやライブラリー化してオープンなかたちに格納する道筋をつくることを目標にしていますので、フィールドや実社会における臨床研究が大切だと理解しています。

生体情報の占める領域は今まで述べてきましたように極めて広範であります。NTT MEI Labsは生体情報の基本と思われる以下の3つのアプローチから研究に取り組みます。

- ① 生体情報のセンシングと予知、診断、予防、治療のデザイン
- ② 機械学習、Neural Network等による生体情報の解析と基礎

研究

③ 医療や健康のデータベースの基 本構造と社会実装に向けての 研究

研究の遂行にあたっては北米に位置する地の利を活かして、グローバルスタンダードへの迅速な対応、国内若手研究者と北米や世界の若手研究者との切磋琢磨の研究環境の醸成を併せてめざす所存です。幸い、NTTがめざすSmart Worldの実現に向けて提唱する11分野の技術革新のうち少なくとも7つの分野について、NTT MEI Labsは課題の提案やその実現に向けて貢献できる潜在力を持っています⁽²⁾。Bio Digital Twinsの実現⁽¹²⁾は、的確なりアルタイム診断と質の高い治療に欠かせぬ夢の世界ですが、NTT MEI Labsの到達目標として研究を進めたいと思います。

■参考文献

- (1) <http://www.amia.org/inside/stratplan/>
- (2) <https://www.ntt.co.jp/news2019/1905/190509b.html>
- (3) <https://www.mhlw.go.jp/shingi/0112/s1226-1.html>
- (4) https://www.ppc.go.jp/files/pdf/290530_personal_law.pdf
- (5) https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=429AC0000000028
- (6) https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=426AC0000000048
- (7) 神里：“情報技術におけるELSIの可能性：歴史的背景を中心に,” 情報管理, Vol.58, No.12, pp.875-886, 2016.

- (8) <https://nam.edu/programs/value-science-driven-health-care/learning-health-system-series/>
- (9) https://datascience.nih.gov/sites/default/files/NIH_Strategic_Plan_for_Data_Science_Final_508.pdf
- (10) http://www.soumu.go.jp/menu_seisaku/hakusyo/index.html
- (11) N.H. Shah and J.D. Tenebaum: “The coming age of data-driven medicine: translational bioinformatics’ next frontier,” J. Am. Med. Inform. Assoc., Vol.19, pp.e2-e4, 2012.
- (12) <https://www.ntt-research.com/2019/07/08/world-class-research-center-opens-in-palo-alto/>



友池 仁暢

「新しく研究所が情報科学・技術の世界の震源地に誕生する」、聞いただけでワクワクしませんか。近代日本は開国と同時に通信と医療を国の根幹の1つに掲げ、それぞれの取り組みが始まりました。150年余を経て、“通信”の営みの中に医療の基礎研究が取り上げられることになりました。それも、量子計算、暗号の研究所と同時に動き出すわけで、21世紀全体を見渡した大事業です。Sustainableで豊かな世界への強い願望を現実のものにできるように研究を進めます。

◆問い合わせ先

NTT Research, Inc.
NTT MEI Labs
E-mail info@ntt-research.com

2019年の暗号研究所開設にあたって

NTTは2019年7月1日、大規模な組織再編の一環として、シリコンバレーにNTT Research, Inc. を設立しました。NTT Research, Inc. は、暗号、量子コンピューティング、ヘルスケアの3つの研究所で構成されており、それぞれの研究所は日本から来られた著名な方によって運営されています。私は暗号研究グループに加わることにとても興奮しています。私はこの取り組みを始めるにあたり、何人かの研究者を募集しました。本稿では、企業研究所を成功させるための私の考えを紹介します。

Brent Waters

NTT Research, Inc.

はじめに

新しい研究所を立ち上げようとする熱意には多くの理由がありますが、同時に、この取り組みが直面している課題を考えることも重要です。私のキャリアの中で、いくつかの活発な暗号研究グループを見てきましたが、それらのグループがもはや存在しないことが気になります（本稿で「研究」という言葉を使うのは、ある分野のトップカンファレンスやジャーナルで発表される基礎研究のことです）。私の最初のインターンシップは2003年の夏で、当時少なくとも6人の暗号学者を雇っていたPARCで働いていました。それから何年もたたないうちに、彼らは皆去ってしまいました。シリコンバレーのMicrosoft Researchは、暗号技術をはじめとするコンピュータサイエンス分野の著名な研究者を抱えた一流の研究所とみなされていましたが、2014年9月に突然閉鎖されました。ごく最近では、準同型暗号の発明などで知られるIBM Researchの暗号研究グループが、2019年の春に一斉に去ってしまいました。

もちろん、時間の経過とともにある程度の変化や離脱は避けられないもの

ですが、コンピュータ科学の研究室は大学の学部に比べて永続性が低いように思われます。基礎研究においてほとんどすべての企業研究所が直面している問題の1つは、企業に対して生み出すビジネス価値を最終的にはっきりさせなければならないという圧力ですが、これには課題が伴います。第1に、多くの分野におけるもっとも優れた研究は、より長い時間軸で影響を与えるもので、企業の短期的な目標と整合させることが困難な場合があります。第2に、どのようなグループからの優れた研究であっても、公開され、組織外の人々からの研究の上に積み上げられ、他のグループや組織によって利用されます。これは典型的には、強力な研究グループを構築することの利益が暗黙のうちに広範なコミュニティと共有されることを意味します。もちろん、社外での出版や共同作業を切り詰めることは1つの方法ですが、少なくとも私の分野では、私はそのアプローチが最高品質の研究を生み出すとは思っていません。企業は、強力な研究グループを持つことによって、逆に外部の研究者のイノベーションにも立ち会い、それを活用することができるのです。

これらの課題があるにもかかわらず

ず、適切な方法をとることができれば、新しい研究室を立上げ、参加する機会には、研究者にとっても組織にとってもリスクをはるかに上回る価値があります。成功する研究所をどのように構築するかについて以下に述べます。私がここで共有する視点は、コンピュータサイエンスにおける一流の文献を生み出すこと、すなわち「最高の」研究の創出を第1目標とする研究室をつくることです。これらのアイデアのいくつかは、異なる目標に対しては異なる運用がされるかもしれません。

エリートになる

「正しくやるか、さもなくばやめなさい」それなりの研究所を立上げるのは簡単ですが、偉大な研究所をつくることは挑戦と興奮を生むものです。

これは適切な人材を雇用することから始まります。一流の研究者と平均的な採用者との差は極めて大きいものです。したがって、最高の人々を引きつけるための戦略を立てることは理にかなっています。良い出発点は給与と報酬です。優秀な人材を獲得することに大きな価値の差があることを考えれば、適切な人材を獲得するために必要なことは何でも行うべきです。チーム

が1人のスーパースターを獲得するために、複数の選手とトレードすることに熱心になるプロスポーツは1つの比較ポイントでしょう。報酬のための資源は有限です。量より質を重視することを私は提案します。

トップ研究者は互いに協力したいと思うでしょう（反対に、適切な人材を採用しないことは、将来の採用活動の障害にもなりかねません）。企業の研究所でできることの1つは、複数の人が共同で作業できる環境をつくることです。これはインターンやポストドクターの採用にも有効です。もしあなたが必要な数の上級研究者を確保できれば、この研究室は大学院生が夏の間に群がる目的地となるでしょう。

研究者に得意なことをさせましょう

幸運にも適切な人材が得られれば、彼らがもっとも得意とすることをさせましょう。トップ研究者は特別な能力を持っていて、基礎研究に集中したいと思っています。それらを管理する最善の方法は、「彼らのことをする」ためのスペースを与えることです。もちろん、彼らのアイデアを実用化しようとしている開発者に、彼らのアイデアを説明してくれるよう研究者に時々頼む、といったようなことは理にかなっています。そして、ほとんどの研究者は喜んでそうすることでしょう。しかし、研究者が何をすべきかというグループのビジョンが、研究者が得意なことをやり通すことと大きく異なるの

であれば、そのビジョンは当初から基礎研究と両立しないと私は主張します。

また、研究者が研究に費やす時間を確保することも重要です。追加のミーティングやその他のオーバーヘッドを伴うアクティビティの量を最小限に抑えることが重要です。外部の方々が研究室の成果に触れることは重要ですが、その多くは、研究者が学会や招待講演で論文を発表することで自然に行われます。一般的に、研究者は自分の時間をどこで過ごすのがもっとも良いか、すでによく知っているものです。

競争相手と、競争に必要なものを知しましょう

非常に強い研究者を確保するという理念に同意するとしましょう。次に、競合他社について知る必要があります。研究大学の教員職に焦点を当ててみましょう。教員の一人として、研究者は以下のことをするでしょう。意欲的な大学院生と接触する機会を持ち、終身在職権（テニユア）によって生涯の仕事の安定を達成する機会を持ち、彼らの興味を追求することにおいて多くの独立性を感じ、立派な個人オフィスを持つ大学キャンパスで研究を行い、教授として認められる名声を得ようとするでしょう。

すでに大学で職を得ている人や、大学でのポストを考えている新卒博士を採用しようとする際には、この点を念頭に置くことが重要です。もちろん、どうしても代替できないものもありま

す。もし誰かが教職に就きたい、大学のキャンパスにいたい、そして教授と呼ばれたいと思っているなら、彼らには大学での仕事が向いているでしょう。しかし、企業の研究室が学術的な地位に到達し、それを上回ることができるという側面はほかにもあります。まず、オフィススペースから見てみましょう。多くの企業の業務環境には、エンジニアがデスクまたはパーティションで作業する「オープンオフィス」が備わっています。NTT Research, Inc. の採用候補者の多くに（そして私自身にも）話を聞いたところ、このような仕組みは研究者には受け入れられないだろうと確信を持っています。研究者は、アイデアに集中できる個室のオフィスを求めています。これは、コンピュータ科学の教員なら誰でも与えられるものであり、同じものが提供されなければ、求人天秤にかけている誰にとっても重大なマイナスとみなされます。それに加えて企業自体の一定の高い評判（そして、それが無いに伴う名声の欠如）があります。採用者を特別な気持ちにさせたいのであれば、これは非常に重要です。

ほかにも企業の研究所が大学のポストを上回ることができる場所があります。

① 報酬

大学では、給与を比較的均一かつ低めに維持することを求める政治的圧力などがあります。企業の研究所は、理想的には、より多くの費用を支払う能

力と、雇用目標を達成する柔軟性を持つべきです。

② エリア内の同僚の数

NTT Rsearch, Inc. では、同じロケーションで複数の暗号技術者を雇用する機会があります。バランスの取れたコンピュータサイエンス学部では、雇用はさまざまな研究分野に分散してしまします。これは研究所の研究者に特別な機会を与えます。

③ オーバーヘッドの削減

研究所では、授業をする必要も、委員会に参加する必要も、資金を探す必要もありません。純粋な研究により多くの時間を費やす自由は大きな魅力となり得ます。タスクやミーティングを作成しすぎて、この利点が損なわれないようにすることが重要です。

コラボレーションと公開を容易にしましょう

エリート研究機関の成長を妨げる確実な方法は、文献の公開や共同研究に過剰な障壁を設けることです。研究者は、何ら障害なく社外の人と共同研究ができなければなりません。また、研究論文をオンラインで発表したり掲載したりする際の障壁を非常に小さく、もしくはなくすべきです。そうでなければ、優秀な人たちはほかに働く場所を見つけるだけでしょう。もちろん、企業は研究室から出てきた研究を特許化する能力を持つべきですが、これは中核的な研究目標への障害を最小限に抑える方法で行われるべきです。

上記のすべては、適切なリソースと管理スタイルが整っていれば実行可能です。基本的な研究は製品開発とは異なりますし、学問的な研究者は技術者とは異なります。研究所を成功させるためには、企業は明確なアプローチを開拓する必要があります。

おわりに

最後に、画期的な研究を生み出す企業研究所を持つことの多くの利点について述べたいと思います。明らかなのは、新しいアイデアを生み出す研究者は、企業の知的財産ポートフォリオの構築に役立つということです。さらに、社内に専門知識を持つことは、新しい技術を評価するのに非常に役立ちます。しかし、もっとも重要な役割は、研究所が革新的で斬新なアイデアの源であることでしょう。企業がトップを維持するためには、変化と新しいアイデアを受け入れることが必要です。NTTのキックオフ・イベントで私が興味を持ったのは、名前に「電話」と「電信」という言葉を使っている会社にもかかわらず、現在の収益のうち音声（モバイルの音声を含む）によるものは20%にも満たないということです。企業と研究所との関係性を維持するためには、どんな企業も時間の経過とともに進化しなければなりません。研究における大きなアイデアは、予期せぬところから生まれることもあります。例えば、私のもっともよく知られている研究成果の1つは、特定の個人

を対象とするのではなく、ポリシーを暗号化する方法である「属性ベースの暗号化」です。しかし、この概念は、バイオメトリクス認証のための暗号化方法を最初に追い求めていた研究（Amit Sahai氏と）から生まれました。成功した研究所を運営することが企業の将来の成長の柱となるのは、まさに、根本的に新しいアイデアや技術を活用する能力です。



Brent Waters

NTT Rsearch, Inc. の堅実な立上げには非常に勇気付けられ、今後の展開を楽しみにしています。

◆問い合わせ先

NTT Research, Inc.

E-mail info@ntt-research.com