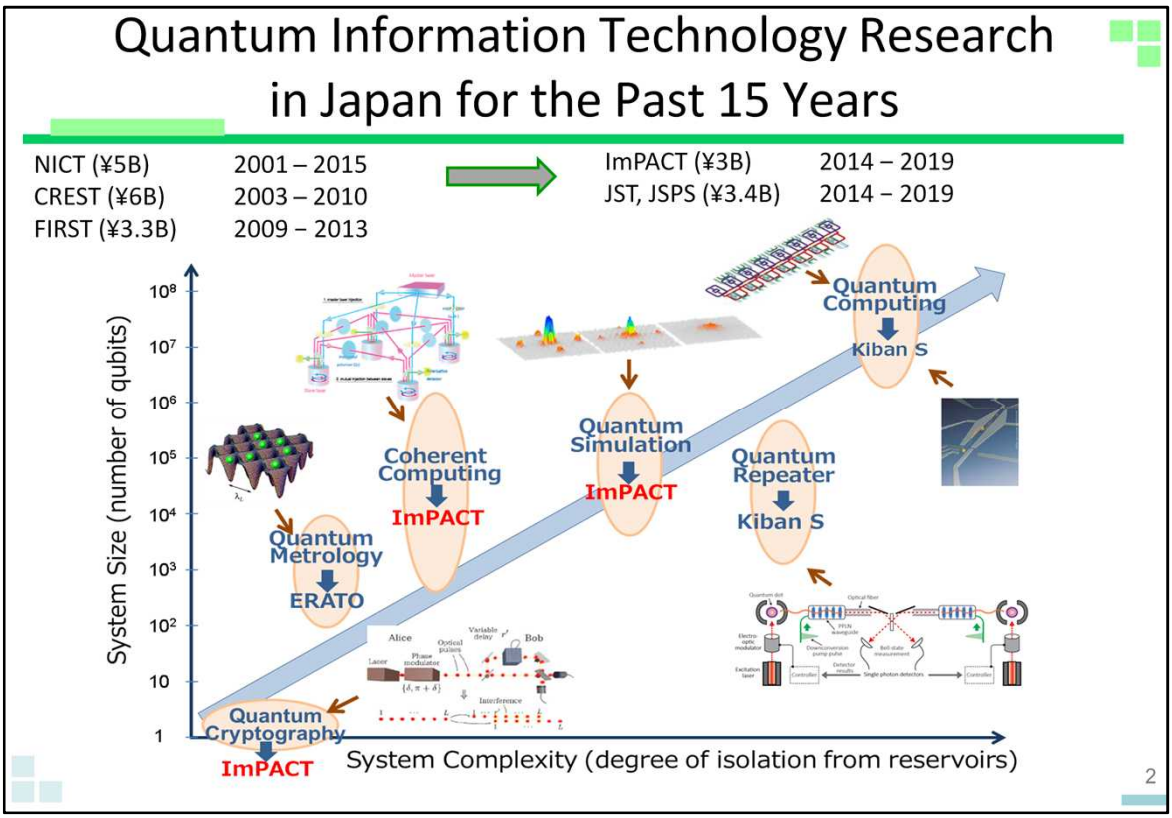
ImPACT Project on Quantum Technology

Yoshihisa Yamamoto

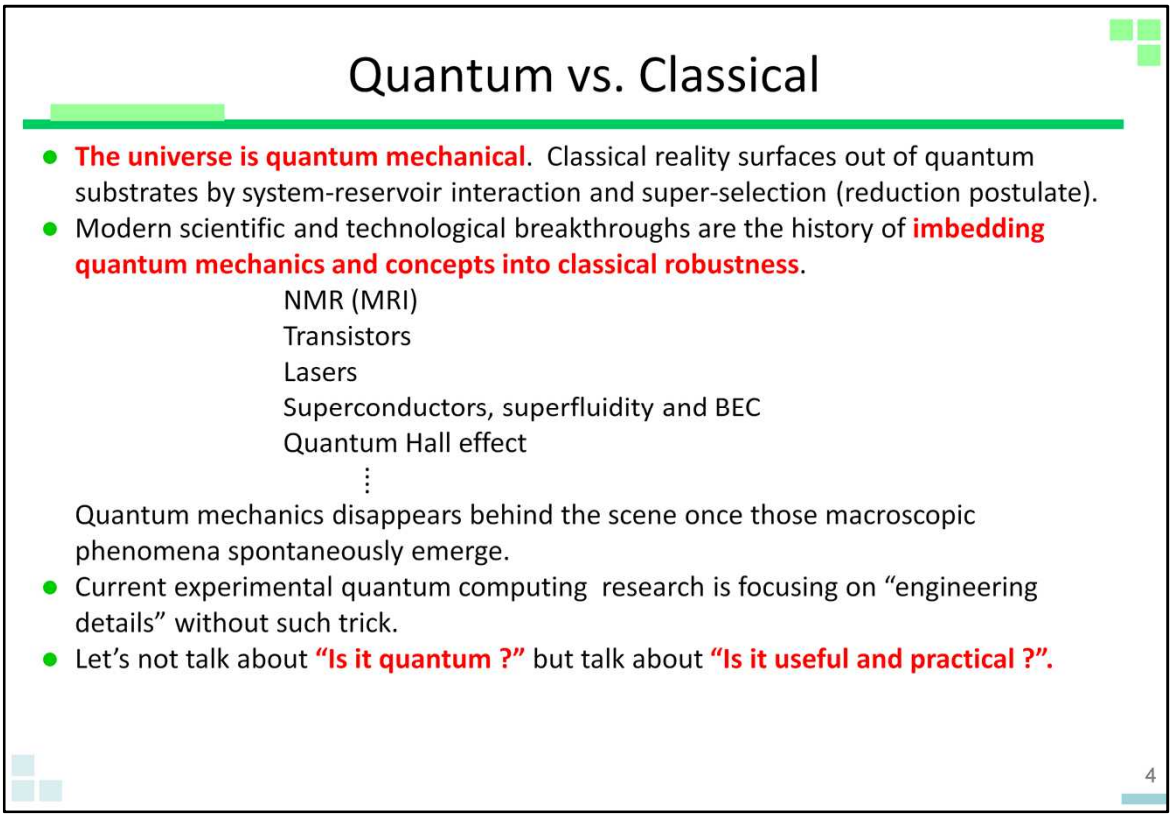
ImPACT Program Manager

Japan Science and Technology Agency

ImPACT量子技術プロジェクトの第1回全体会議のキックオフにあたりまして、この領域の置かれている現状とこのプロジェクトの目指すところをお話しておきたいと思います。私はプログラム・マネージャーを務めます山本です。

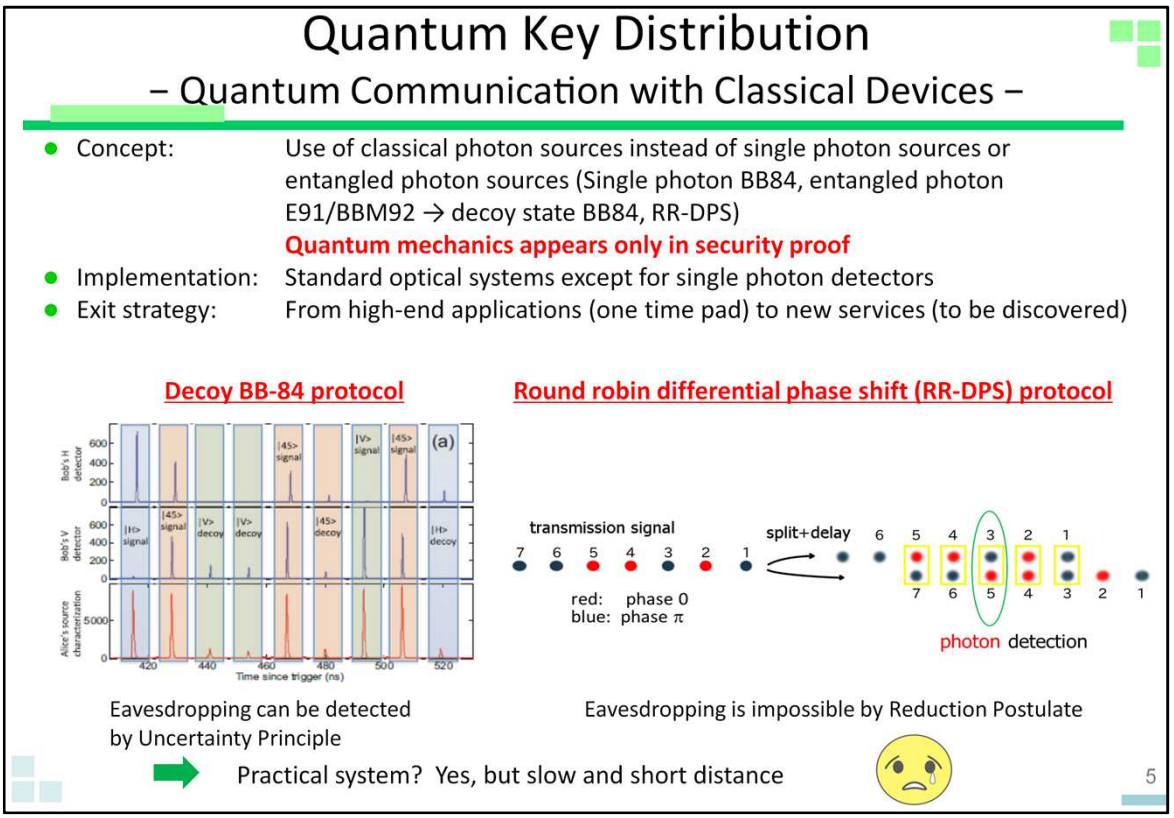


過去15年間に量子情報技術に投下された国家プロジェクトの予算規模と研究テーマをこのスライドにまとめています。総務省（NICT）、文部科学省（JST-CREST）、内閣府（FIRST）などから総額150億円近い研究費が、量子暗号、量子計測、コヒーレント・コンピューティング、量子シミュレーション、量子中継、量子コンピューティングの6テーマに投下されて来ました。このグラフは、システムを大きさ（量子ビット数）を縦軸に、システムの複雑さ（量子ビットを制御する技術の精度）を横軸に取って、これら6つのテーマをプロットしたものです。このうち量子暗号、コヒーレント・コンピューティング、量子シミュレーションの3つがImPACTに引き継がれました。光格子時計をはじめとする量子計測は、国の標準研究所を中心に国際標準化を目指した開発フェーズに入ったことで、国プロから外れました。量子中継と量子コンピューティングは、JSPSやJSTの基礎研究支援制度下で、長期的な研究テーマとして地道な研究を継続すべきものとして、やはり国プロから外れました。



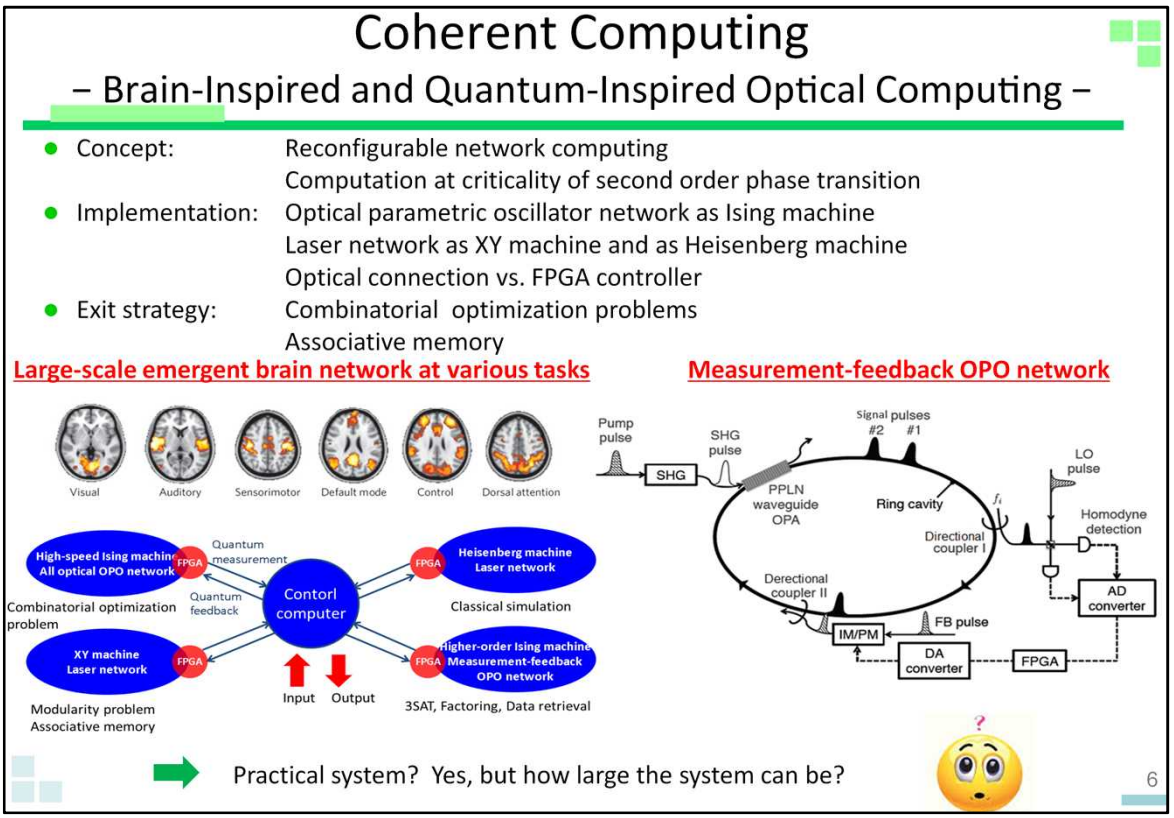
この点に関する私の意見を、このスライドにまとめてあります。

1. 私達は皆この世界が量子力学の法則に支配されている（より正確には量子力学の原理を用いて記述される）ことを知っています。Classical Reality（古典的な実在）というものは、その量子基盤の中からシステム-熱浴相互作用と超選択則を通して例外的に出現します。私達はその古典的な実在の一つであるため、古典を普通のもの、量子を特別なものと考えがちですが、事実はその逆で量子は普通のもの、古典が特別なものなのです。
2. 現代技術のブレークスルーは、量子の原理や基本概念を古典世界の実在に埋め込むトリックとして発明されてきました。NMR (MRI)、トランジスタ、レーザ、超伝導・超流動・ボーズアインシュタイン凝縮、量子ホール効果、などは全てマクロな効果として古典世界に発現した時、その背景にあるミクロな量子性が表舞台から姿を消していることによって、実用性を手に入れたものです。
3. 現在の量子コンピューティングの研究開発では、そうした知恵や基本的ブレークスルーなしに、古典世界に量子力学を実現するための技術的詳細に目を奪われている気が私にはしています。
4. このImPACTプロジェクトにおいては、それは"量子"だから研究する価値があるという考え方を捨てて、それが"役に立つ、現実的な技術か"という問いかけを常にしたいと思います。自分達だけの狭い世界に閉じこもって、一人よがりに研究を正当化するのを止めて、外の世界に目を向けた研究姿勢が要求される時代です。



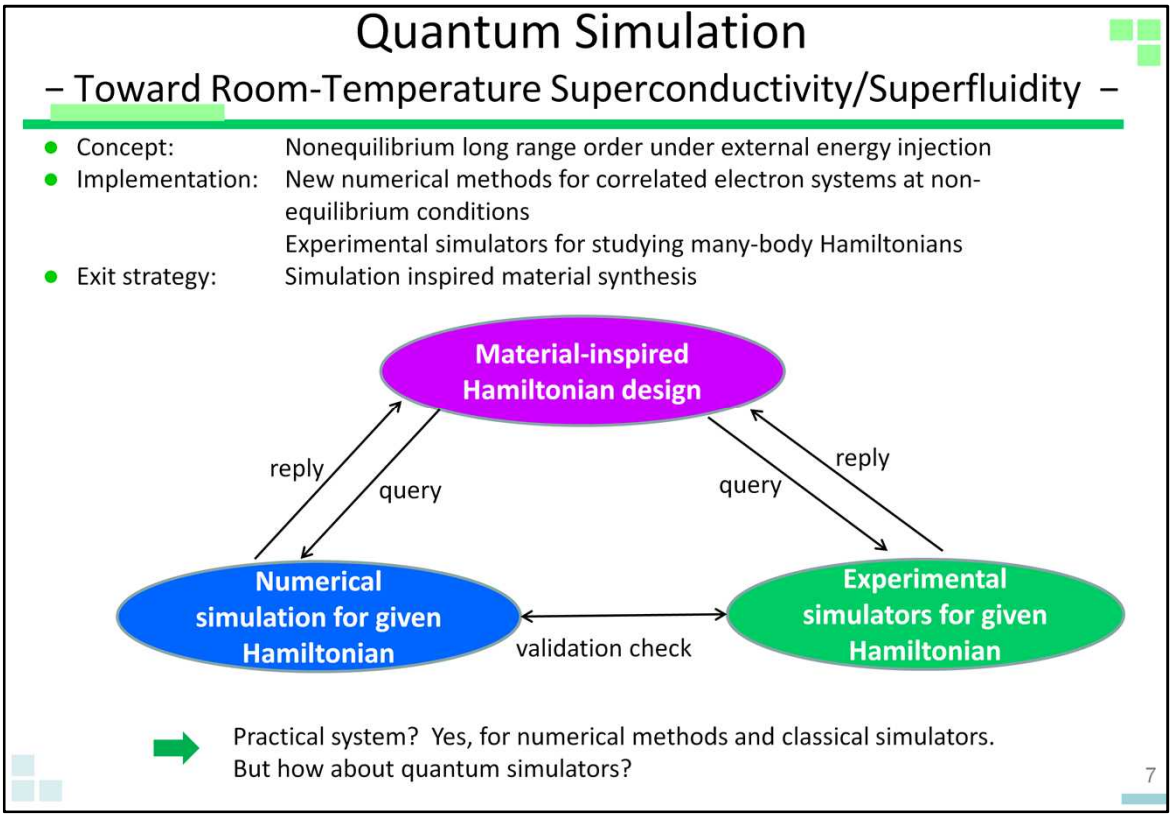
次に、ImPACTで取り上げる3つの研究テーマの現状を分析します。
まず、量子暗号の分野について述べます。この分野が実用技術に１歩近づけたのは、物理的システムのどこにも量子力学が登場しないからです。当初は、単一光子を用いたBB84プロトコルやエンタングル光子対を用いたE91/BBM92プロトコルの実装が模索されましたが、現在では通常のレーザ光源で実装されるdecoy BB84プロトコルやRound Robin DPSプロトコルというものが発明されました。これらのシステムでは、量子力学は安全性証明の数学の中に現われるだけで、現実のシステムは通常の古典デバイスだけで構成され、量子の中核的概念である量子エンタングルメントはどこにも存在しません。そのため、ある程度実用的なシステムを組むことができました。しかし、量子暗号には深刻な弱点も残っています。その弱点とは、

1. one-time padと組み合わせた方式は、鍵配送速度が極めて遅く、伝送距離も短く、この点現代暗号に比べて全く不利な状況にあります。盗聴者の能力に限界を仮定しない“絶対安全性”を売りにしてきたわけですが、盗聴者の能力限界よりもより現実的なシステム構成要素の不完全性に起因する“安全性脅威”の問題がまだクリアされていません。high-endの応用分野をターゲットに置くとしても、この点がクリアされなければユーザに対しての説得力はありません。
2. 小さなスタートアップ企業であれば、量子暗号実験を行なう大学の研究室に小規模な装置を売るビジネスモデルが成立するのでしょうが、日本を代表する大企業の場合にはより大規模な市場が将来形成されなければビジネスとして成立しません。この点、送受信装置のコスト低減に向けた努力だけでは不十分で、bright pulseが伝送されている光ファイバー伝送路に波長多重で単一光子レベルの量子暗号チャンネルを挿入して、十分なS/N比が実現できる技術の開発が不可欠であります。量子暗号のためだけに光ファイバー伝送路を専用線として使うというオプションはないと考えるべきです。
3. 1024ビットの因数分解を用いたRSA公開鍵暗号が将来破られた場合を想定した現代暗号の代替技術（ポスト量子現代暗号）の研究が進展しています。この強力なライバルに対して、長期的視野に立って量子暗号の勝ち目、適用分野を見通しておく必要があります。



コヒーレント・コンピューティング（量子人工脳）は、脳における情報処理と量子を用いた情報処理の融合を目指す新しい光コンピューティングです。まず、量子コンピューティングの最も重要なリソースは連続位相を利用した干渉効果にあり、最大の弱点は非局在波動関数実現のために量子エンタングルメントというひ弱な要素を導入せざるをえなかった点にある、という基本認識が背景にあります。そこでエンタングルメントを使わずに非局在波動関数と干渉効果を実現する光子を情報キャリアに用いて、デコヒーレンスの問題を解決します。こうして実用性を獲得しました。次に脳における情報処理の強みとして、目的に応じてネットワークを再構築して、その都度最適なコンピュータを実現していること、状態を常に相転移の臨界点に設定して、自発ゆらぎを大きくゆっくりしておき、外部からの入力に対して瞬時にマクロな秩序（オーダー）を形成できる準備をしていること、という基本指針があります。後者を実現するため、レーザや光パラメトリック発振器（OPO）の２次相転移の臨界現象を計算過程に使います。また前者を実装するため、DOPOネットワークをベースにしたイジングマシーン、レーザネットワークをベースにしたXYマシーン、NDOPOをベースにしたハイゼンベルグマシーンなど異なる機能を持つネットワークを目的に応じて再構成できるようにします。こうして、組み合わせ最適化問題や連想記憶メモリーなどへの応用を目指します。kmオーダーの光ファイバーリング共振器に多重パルスOPOやレーザを実現することにより、1万～100万のノード数を持つグラフが小型な装置に実装できます。しかし、このコヒーレント・コンピューティングには克服すべき課題が残っています。その課題とは、

1. 1万～100万のノードで完全グラフを構成するためには、1億～1兆というエッジを張らなければなりません。提案された量子人工脳では、これを光ホモダイン検波回路とFPGA/ASICデジタル電子回路を用いた量子測定フィードバック回路で実現しようとしています。これだけ大規模なFPGA/ASICを高速で動作させることが本当にできるのか、は決して自明なことではありません。
2. 同じ組み合わせ最適化問題を解くヒューリスティック（焼きなまし法：SAなど）、量子アニーリング、CMOSアニーリング（日立）などとの性能比較（ベンチマーク）を行い、量子人工脳の適用分野を見通しておく必要があります。
3. ノード数1億～10億、エッジ数10京～100京のグラフを実装するためには多数の量子人工脳を並列動作させなければなりません。この並列動作をサポートする通信路をどう確保するのか、見通しを持っておく必要があります。



最後に量子シミュレーションの分野について述べます。
この研究テーマの最終目標は、室温超伝導体など材料科学のブレークスルーの実現に向けたシミュレーション・ツールの開発です。一言で目指すところを言えば、“材料研究者の直感に頼らない科学的材料開発”に役立つツールの開発です。そのためには、現実の物性に根ざしたハミルトニアンの提案、これを数値シミュレーションするソフトウェア、その手法を実装するハードウェアの開発を同時に行なっていく必要があります。特に、外部からのエネルギー注入や外部へのエネルギー散逸がある非平衡下でのボーズアインシュタイン凝縮を扱える理論的・実験的手法の開発が必要です。この研究テーマにおいて、進むべき方向は、

1. 室温超伝導・超流動につながる物質と物性を特定し、量子シミュレーションのターゲットとなるハミルトニアンを明示する。
2. その目標となるハミルトニアンを十分な近似精度で数値シミュレーションできる手法を開発し、発現する物性を予測する。
3. その数値シミュレーション手法の背景にある重大な仮定を明確にし、その点に特化した実証実験を企画し、実行する。

の３つであります。
量子シミュレーションの研究にとって最も危険なことは、実証実験をする必要がない自明なことをシミュレートする実験を行うために大切なリソースを投下することです。理論モデルのどの部分に確信を持てないかで実験を計画する必要があります。

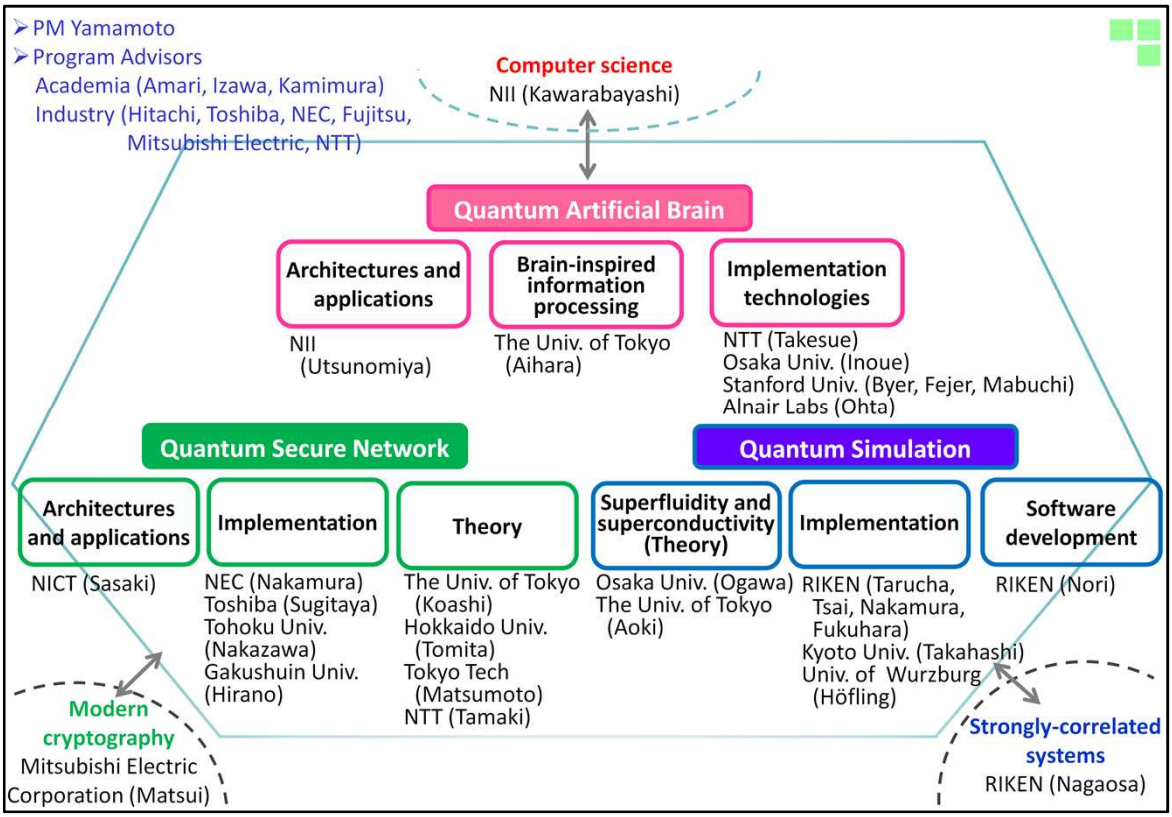
Basic Strategies in ImPACT Project

Three frontiers: Computer Science
Modern Cryptography
Strongly Correlated Physics

Theoretical efforts: Imbedding quantum concepts in the theoretical model and the numerical methods for modern digital computers **(creative quantum software)**

Experimental efforts: Development of simple and practical quantum technologies **(robust quantum hardware)**

量子情報技術の実用化・商品化を考える時、出口で対峙している3つの領域で何が課題なのかを十分に分析しておく必要があります。３つの領域とは、計算機科学、現代暗号、強相関電子物性、です。これらの領域で何が問題で、量子はどうその問題解決に寄与できるのか、を明確にしていく予定です。
理論サイドでは、量子の概念を理論モデルに埋め込み、現代のデジタルコンピュータでこれを解けるようにすることが目標です。（“creative quantum software”）
実験サイドでは、シンプルで実用的な量子技術の開発を目指します。（“robust quantum hardware”）



最後に、プロジェクトの体制をこのスライドにまとめました。
3つの出口である計算機科学、現代暗号、強相関電子物性の国内第一人者である河原林（NII）、松井（三菱電機）、永長（理研）にプロジェクトに参加していただきました。この3人を納得させられない量子技術には、社会へ出てゆく可能性はないと覚悟を決めて研究開発に取り組むことになります。
量子セキュアネットワークの研究開発では、佐々木（NICT）が全体を統括します。中村（NEC）と井上（東芝）が量子鍵配送の装置・システム開発に取り組み、中沢（東北大）と平野（学習院大）が光ホモダイン検波／デジタルコヒーレント伝送技術の導入による高性能化に取り組みます。現実的デバイスの不完全性による安全性への脅威の解析を、小芦（東大）、玉木（NTT）、富田（北大）が担当します。松本（東工大）は量子暗号の欠点（低速・短距離）を克服する手法の探索を行ないます。
量子人工脳の研究開発では、宇都宮（NII）が全体を統括します。合原（東大）は、脳型情報処理の概念を量子人工脳の原理と応用に展開する取り組みを行ないます。武居（NTT）、Fejer/Byer/Mabuchi（スタンフォード大）は、OPOネットワークの開発に取り組みます。太田（アルネア）はレーザネットワークの開発を担当します。井上（阪大）がNCOSを使ってFPGA開発に取り組みます。
量子シミュレーションの研究開発では、小川（阪大）、青木（東大）、西森（東工大）がターゲットとなるモデルハミルトニアンの提案と数値シミュレーション手法の開拓、Nori（理研）がその成果をインターネットを介してfree softwareとして配信する計画です。これが出口戦略の一つの形です。数値シミュレーション手法の有効性をチェックする実験装置の開発を、高橋（京大）、樽茶／中村／蔡／福原（理研）、Höfling（ウルツブルグ大）が担当します。
プロジェクト内から研究開発の方向性をチェックしていただくため、甘利（理研）、伊澤（千歳科学技術大）、上村（東京理科大）、川上（京大）の４名の先生方にプロジェクト顧問になっていただきました。また、プロジェクト外からは、日立、東芝、NEC、富士通、三菱電機、NTTの６企業の研究開発部門を統括される立場の方に、それぞれアドバイザーになっていただきました。研究テーマとアプローチに関して、産業界からのフィードバックをいただく予定です。
以上の体制で、これから４年間ImPACTプロジェクト研究を行っていくことになります。日本の量子情報技術に与えられた数少ないチャンスです。是非、皆様と一緒にこの機会をものにして、日本の存在感を世界に示したいと考えています。