

「量子力学的効果の情報通信技術への適用とその将来展望に関する研究会」報告書概要

第 1 章 量子情報通信について

量子情報通信の可能性

情報通信技術の急速な進歩

- インターネット人口の急増、携帯電話の急速な普及
- 電子商取引等の新しい情報通信サービスの展開



高速化、高信頼化の要求増大

電気や光の波としての性質を利用した現在の情報通信技術→ 早晚、物理的限界



ブレークスルーが必要

量子情報通信技術

「量子重ね合わせ(*)」、「観測による射影(*)」及び「量子もつれ合い(*)」という3つの基本的性質を用い、情報を送る信号を電子や光子などの量子力学的レベルにおいて処理する技術



量子情報通信の可能性

- 絶対に解読不可能な暗号通信 [量子暗号]
- Shannon の定理 (注) の限界を打破する超高速通信 [量子通信]
- 現在のスーパーコンピュータの能力を凌駕する超並列・高速情報処理 [量子コンピュータ]

(注) Shannon の定理：外部雑音や通信誤りを考慮した現在の情報通信技術の最大伝送速度を表す法則。

【参考】インターネットの基本技術は、30年前の実験的コンピュータネットワークの運用・研究開始以来、米国政府の手厚い先行投資があった。米国経済は、この先行投資の恩恵を30年後の今、享受している。

*：別添2の「用語解説」参照

第2章 国内外の研究開発動向

量子情報通信技術の研究開発動向

1 量子暗号

理論研究：複数の量子暗号鍵配布プロトコルの提案。

実証実験：伝送速度 数百 bps、伝送距離 数十 km 程度の鍵配布実験に成功。

2 量子通信

理論研究：Shannon の定理に代わる量子符号化の基本定理の一部が確立。

実証実験：量子テレポーテーション^(*)の原理の実証等、海外の基礎的実験の成功を機に国内外において研究が活発化。

3 量子コンピュータ

理論研究：素因数分解、データベース検索等の量子計算アルゴリズムの提案。

実証実験：基本的な回路を構成する固体素子を開発中。

4 デバイス開発

半導体を用いた量子ゲートなど、量子情報通信の実現に必要な基本素子を開発中。

日米欧の研究開発動向（国家プロジェクト関連）

1 米 国

■ NSF（全米科学財団）

…公募研究制度により、研究開発を推進。（最近4年間で約33億円）

■ DARPA（米国国防省高等研究計画局）

…3年～5年間の研究プロジェクトを推進。

■ NIST（米国標準技術局）

…独自の研究部門により、量子デバイス等の研究開発を実施。

■ NSA（米国国家安全保障局）

…HPCC(High Performance Computing and Communications)（注）において、量子暗号等の研究開発を推進。

（注）HPCC：米国の情報通信関係の研究開発プログラムで、NII(National Information Infrastructure)の一部に位置づけられている。HPCCは、5つのプログラムにより構成されており、より高性能なコンピュータ、より高速なコンピュータネットワーク、より高度なソフトウェアを作り出すための研究開発に対して資金を投じるもの。

2 欧州（EC）

- 1984年の第1次フレームワーク開始以来、量子情報通信分野の研究開発を実施。現在は、第5次フレームワーク（1998年～2002年）の下、1999年より12の研究プロジェクトを集結した研究コンソーシアムを構築し、研究開発を推進。（研究資金は、4年間で約22億円の予定。うちEC負担額約17億円。）

3 日 本

- 公的研究機関、大学、民間企業において個別に細々と研究が行われており、総合的かつ戦略的な取組はなされていない。

第3章 量子情報通信の将来予測

量子情報通信システムの実現までには不確定要素が多く、正確に将来像を描くことは難しいが、必要な理論やデバイス等が全て開発された場合の実現イメージは以下のとおり。

【量子情報通信の技術開発ロードマップ…別添1】

1 量子暗号

自宅のパソコンからインターネットで決済しても、途中でパスワードやクレジットカード情報が盗まれる心配が全くない通信が実現

2004～2010年頃：比較的短距離（～数十km）での量子暗号鍵配布が実現

2010～2030年頃：汎用のセキュリティシステムに拡大した量子セキュリティシステムが実現

2 量子通信

多数の量子コンピュータ間等を量子暗号によりセキュリティが確保された情報が自由に往来する、量子通信ネットワークが実現

2007～2020年頃：量子通信のプロトタイプの実現

2010～2030年頃：限定用途での量子通信が実現

2030～2100年頃：空間伝送も含めた量子通信ネットワークに発展

3 量子コンピュータ

現在のスーパーコンピュータの能力をはるかに凌ぐ超並列・高速情報処理が実現し、例えば、スーパーコンピュータで1年かかる計算をわずか0.1秒で処理。（暗号鍵を容易に解読）

2010～2030年頃：素因数分解、データベース検索等に特化した専用量子コンピュータが実現

2015～2100年頃：汎用量子コンピュータに発展

第4章 取り組むべき研究課題

量子情報理論、量子通信理論の課題

…雑音がある実際の通信路での伝送効率や信頼性の定式化、誤り訂正符号理論の確立等

デバイス開発の課題

■ 短期的課題

…安定してキュービット(*)を生成・検出する単一光子源・単一光子検出器の実現等

■ 長期的課題

…複数のキュービットの量子もつれ合い状態を生成する装置、2光子間の演算を行う光子ゲートの実現等

システム開発・実証実験の課題

■ 短期的課題

…量子暗号鍵配布を実証するテストベッドの構築、各種デバイス高度化、暗号生成ソフトウェア、システム管理技術の確立等

■ 長期的課題

…より高度な量子暗号通信プロトコル、量子もつれ合い状態を用いた高密度伝送の確立等

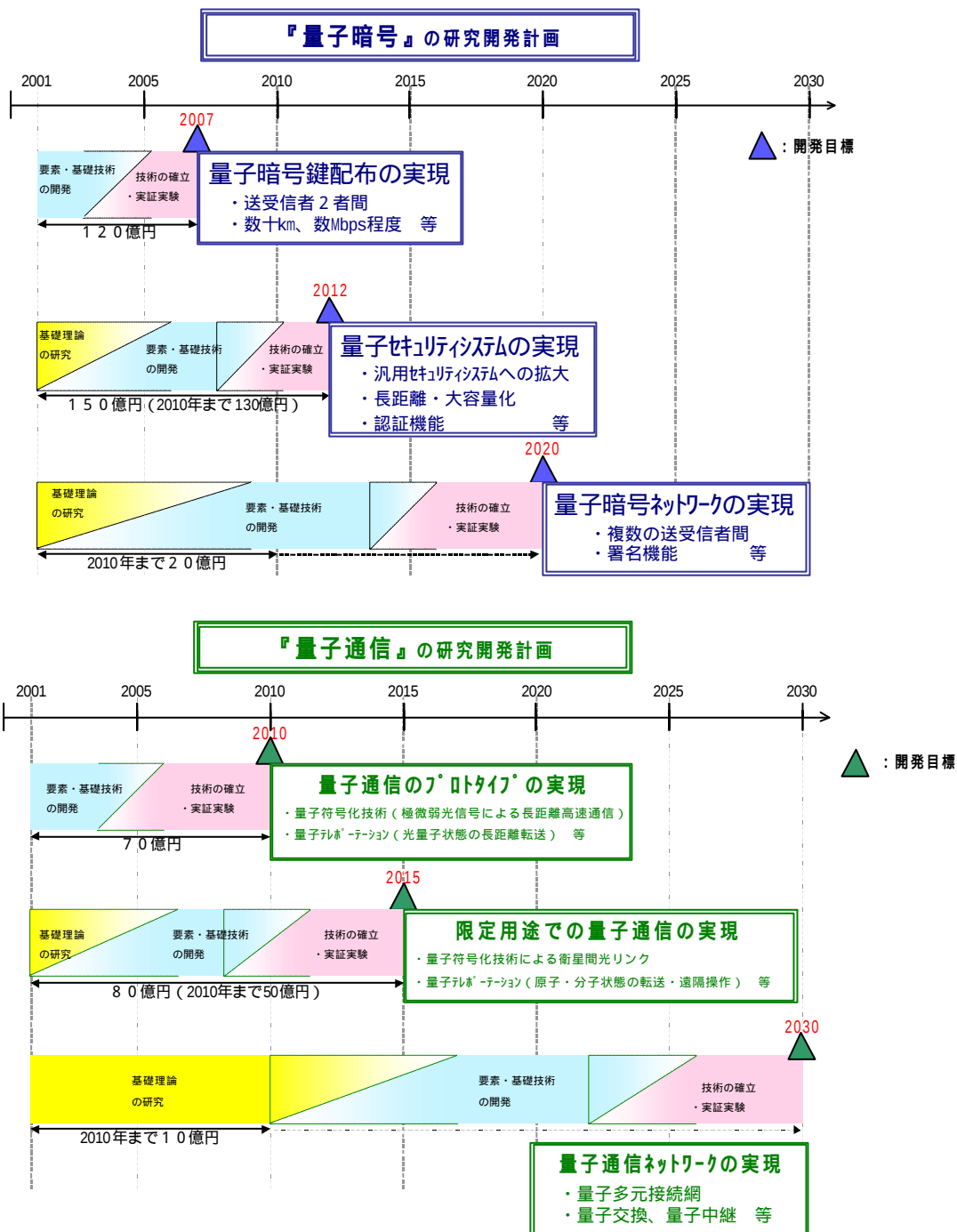
第5章 研究開発の推進方策

計画的な研究開発の推進

我が国において量子情報通信をできるだけ早期に実現するため、以下の研究開発計画に基づいて、理論的研究、デバイスの開発及びシステム開発等を総合的かつ戦略的に実施していくことが不可欠。

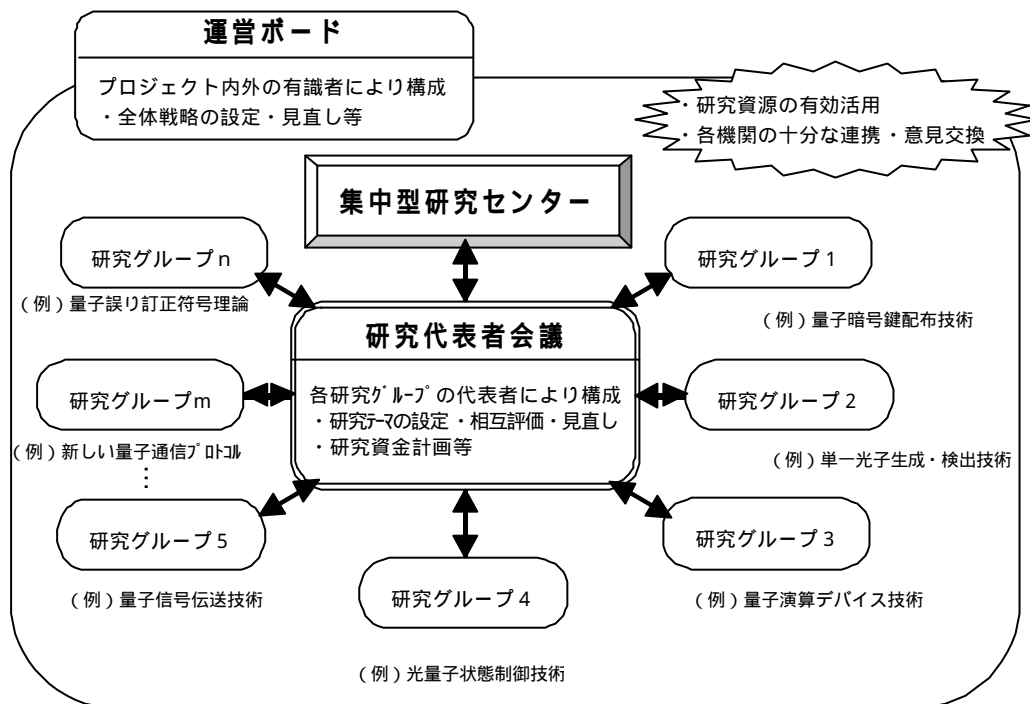
【国が投資すべき研究開発予算 今後10年間：約400億円

（電気通信技術審議会答申「情報通信研究開発基本計画」による）】



研究開発体制

プロジェクト内外の産学官の有識者からなる運営ボードによる全体的な運営・管理の下、中核となる集中型研究センター（各機関から研究者を結集して研究開発を行う環境）と複数の研究グループ（各機関が個別テーマについて少数精鋭で研究開発を行う環境）が有機的に結合した研究開発体制。



考慮すべき事項

上記の研究開発体制の構築のほか、次の措置を講ずることが必要。

- 外国人研究者の招へい制度の有効活用、国際学会への積極的参加
- 期限付任用やポスドク向け助成金制度の改善・拡充
- 精密機器の試作や測定などの専門的技能を持つ研究支援者の確保、処遇の改善
- オープンテストベッドの構築、共通に利用できるデバイス試作環境の整備
- 大学・大学院の研究支援体制の充実
- 公的研究機関としての通信総合研究所のリーダーシップの確保

等