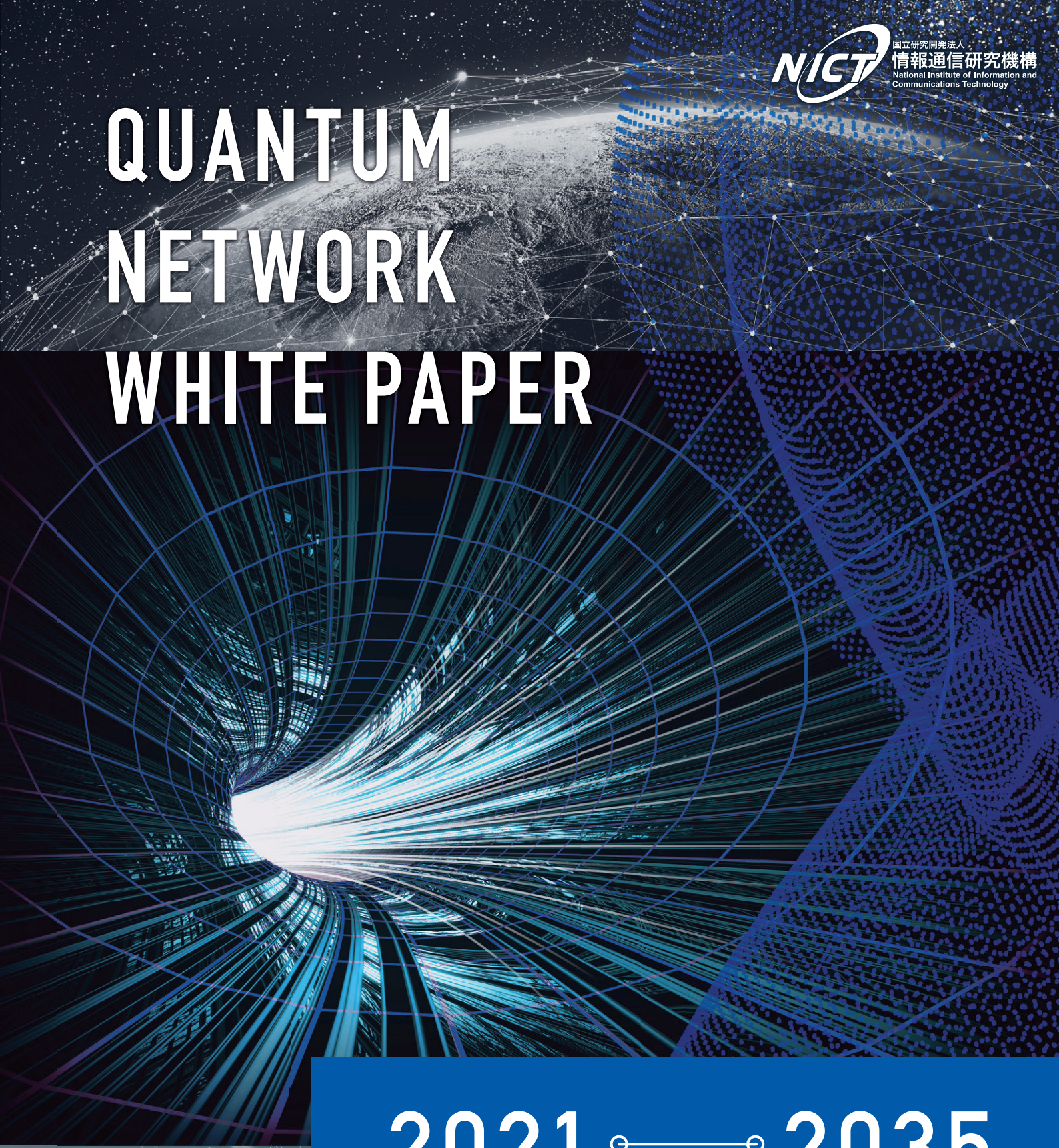
国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

QUANTUM NETWORK WHITE PAPER



2021 — 2035

Table of contents
目 次

01 第1章 はじめに

1．ホワイトペーパーについて

（1）目的

現在、国内外において量子暗号や、さらにその先の量子ネットワーク（究極の目標として「量子インターネット」）に向けた取り組みが進んでいます。日本では 2020 年 1 月に「量子技術イノベーション戦略」が公表されました。NICT は同戦略における「量子セキュリティ拠点」として、量子ネットワーク関連の最先端の研究開発を推進してきているほか、2020 年度より産学官協創の拠点づくりや人材育成の取り組みを開始しています。

本ホワイトペーパーを公表することで、量子セキュリティ拠点としての NICT の研究開発・展開の方向性や今後取り組むべき課題を示すことで、国内外の研究者を惹きつけ、国内外の研究機関との連携を進め、量子ネットワークに向けた研究開発を加速したいと考えています。

（2）ホワイトペーパーの位置づけ

本ホワイトペーパーは、量子通信に関する国内外の動向、量子ネットワークが実現する社会像・ユースケース、その実現に向けて NICT が取り組む研究開発・ロードマップ、推進戦略などから構成されています。本ホワイトペーパーは第 1 版として公表するものです。

本ホワイトペーパーが目指す究極の目標として「量子インターネット」を見据えています。その実現に向けて、国内外の様々なステークホルダーの連携、研究開発などの取り組みの重要性を理解いただくために、想定している読者層として、政府、企業、大学、研究機関等、幅広い方々を想定しています。

（3）検討体制・スケジュール

本ホワイトペーパーは、2020 年 11 月から 2021 年 3 月の 5 か月間、NICT の量子 ICT、未来 ICT、宇宙通信、ネットワークの研究者や、量子ネットワークの推進に取り組む NICT の関係者が議論して取りまとめたものです。

2．国内外の動向と量子情報通信の全体像

（1）量子情報通信に関する全体像

インターネットに代表される情報通信技術は世界の経済・社会の発展を支えるとともに、産業の競争力の源泉となっています。現在は、コロナ禍においてデジタルトランスフォーメーション（DX）の真っただ中にあり、情報通信ネットワークを活用することにより社会の変革が進んでいます。

一方で、情報通信ネットワークにおけるサイバー攻撃は増加の一途を辿っており、安心・安全な情報通信インフラの実現が求められています。

現代の情報通信ネットワークにおいて使われる現代暗号は、米国の大手 IT 企業などにより開発が進められている量子コンピュータが高性能になることによって危殆化することが危惧されており、米国の国立標準技術研究所（NIST）では耐量子計算機暗号の検討・評価などが行われています。また、現在の情報通信ネットワークを流れる暗号化データを盗聴・入手し、高性能な量子コンピュータが実用化した際に解読する攻撃（harvest now, decrypt later）が行われることも危惧されています。

01 第1章 はじめに

そのため、いかなる計算機でも原理的に解読不可能な「情報理論的安全性」を実現する技術として量子暗号が必要とされており、我が国のほか、米国、欧州、中国などを中心に、研究開発や実用化に向けた実証、実運用に向けた量子暗号ネットワークの構築が急速に進められています。

現在、世界各国で研究開発の取り組みが開始された「Beyond 5G/6G」においては、その機能の一つの要件として、「超安全・信頼性」が掲げられており、ここでも量子暗号が重要な役割を果たすことが期待されています。

また、現在、国内外において量子コンピューティングや量子センシング技術の研究開発が進められていますが、将来、こうした技術が実用化して量子ネットワークに接続され、超大規模な情報処理や超高精度な情報収集などが可能になると期待されます（第２章参照）。こうした、量子情報機器・デバイスが量子ネットワークに接続されたいわゆる「量子インターネット」を目指し、欧米などでは基礎研究が進められています。

量子インターネットは、これまでにはない新しいアプリケーション・サービスを実現し新たな社会基盤となることが期待されており、量子ネットワークの研究開発と社会実装に向けた取り組みは、国家の経済・社会の繁栄や安全保障の確保に直結する重要な取り組みとなっています。

（２）量子情報通信をめぐる国内外の政策・研究開発動向

米国、欧州、中国等の諸外国は、戦略的な基盤技術として、量子鍵配送・量子ネットワークを含む量子情報通信に関する研究開発戦略を策定し、大規模な研究開発投資を行うとともに、研究開発拠点形成や人材育成等の戦略的な取り組みを展開しています。

① 米国の政策・研究開発動向

米国では「国家イニシアティブ法」（2018 年）に基づいて、5 年間で 12 億ドルを投じ、サイエンス・ファーストの方針の下、長期的な視点で量子情報科学の研究開発を進めています。その中でエネルギー省（DOE）、国立科学財団（NSF）は、大学、企業などと連携し、量子インターネットの実現に向けた要素技術の研究開発・実証や人材育成を進めています。 科学技術政策局 (OSTP) は、「米国の量子ネットワーク戦略的ビジョン」（2020 年 2 月）において、量子インターネット構築に係る目標・集中すべき 6 つの研究活動領域と次の 5 年及び 20 年の目標を定めています。DOE は「量子インターネット・ブループリント・ワークショップ」を開催（2020 年 7 月）し、量子インターネットに向けた研究開発の方向性やマイルストーンを取りまとめています。

② 欧州の政策・研究開発動向

欧州では、欧州委員会が「量子フラッグシップ」（2018 年～）において、5 年間で 10 億ユーロを投じることとし、量子技術の研究開発に取り組んでいます。また、2020 年 3 月には、量子インターネットを究極の目標とする「量子技術の研究戦略アジェンダ」を公表し、研究開発・産業化・標準化・人材育成に向けたロードマップを公表しています。また、欧州 25 か国が、量子インターネット網の構築に向けた量子ネットワークテストベッド網「EuroQCI」の構築に合意しているほか、「OpenQKD」のプロジェクトにより QKD（Quantum Key Distribution: 量子鍵配送）テストベッドの構築・実証を進めています。

また、英国・ドイツ・フランスなど欧州の各国政府においても、QKD や量子インターネット要素技術の研究開発を推進しています。

01 第1章 はじめに

③ 中国の政策・研究開発動向

中国では、北京－上海を結ぶ量子暗号通信の基幹回線や主要都市に都市圏網を構築し、量子暗号ネットワークの総延長は 2018 年時点で 7,000km を超える規模になっており、その通信機器・デバイス・プラットフォームを提供する多数の企業が設立されています。また、2016 年には人工衛星「墨子号」を打ち上げ、翌年衛星－地上間の量子暗号等の実証に成功しています。2021 年 1 月にグローバルな量子ネットワークの構築に向けて、衛星と地上の統合量子ネットワークの実証を行うことを発表し、天地一体の量子暗号ネットワークの中国全土への展開を進めています。

④ 日本の政策・研究開発動向

我が国では、2018 年より、内閣府において「戦略的イノベーション創造プログラム（SIP）」の第 2 期、文部科学省において「光・量子飛躍フラッグシップ・プログラム Q-LEAP」、経済産業省において量子コンピューティング（量子アニーリングマシンほか）、総務省において衛星通信における量子暗号の研究開発を開始しました。

一方で、これらは関係府省や企業等が個別に研究開発等を行う取り組みとなっており、必ずしも整合性がとられていなかったことから、我が国の産学官の総力を結集して、量子技術イノベーションを推進すべく、「量子技術イノベーション戦略」（2020 年 1 月）が作成・公表されました。

現在、これを踏まえて、8 つの量子技術の研究開発拠点（量子コンピュータ開発拠点（理化学研究所）、量子デバイス開発拠点（産業技術総合研究所）、量子コンピュータ利活用拠点（東京大学－企業連合）、量子ソフトウェア研究拠点（大阪大学）、量子セキュリティ拠点（情報通信研究機構）、量子マテリアル拠点（物質・材料研究開発機構）、量子センサ拠点（東京工業大学）、量子生命拠点（量子科学技術研究開発機構））において、各分野の量子技術の研究開発が進められています。

2020 年からは、内閣府のムーンショット型研究開発制度において量子通信を含む量子技術の研究開発、総務省ではグローバルな量子暗号ネットワークの構築に向けた研究開発が開始されています。

NICT は「量子セキュリティ拠点」として量子暗号やその先を見据えた量子ネットワークの要素技術の研究開発を進めています。

（3）量子暗号

【どんな技術か】

量子暗号は、量子力学の性質を利用することにより、どんな計算機でも解読不可能な暗号通信を実現する技術で、量子鍵配送（Quantum Key Distribution: QKD）とワンタイムパッド（One Time Pad: OTP）暗号化という 2 つのステップから構成されます。QKD とは、理論上いかなる能力をもった第三者（盗聴者）にも情報を決して漏らすことなく対称的な暗号鍵を離れた 2 地点間で共有する方法です。OTP 暗号化では、データ（平文）と同じサイズの暗号鍵を用意し、平文と暗号鍵の排他的論理和によって暗号文を生成します。その際、暗号鍵は使いまわさずに一回一回使い捨てます。これにより、量子コンピュータを含むいかなる計算機でも原理的に解読不可能な「情報理論的安全性」を持った暗号通信を実現することができます。

01 第1章 はじめに

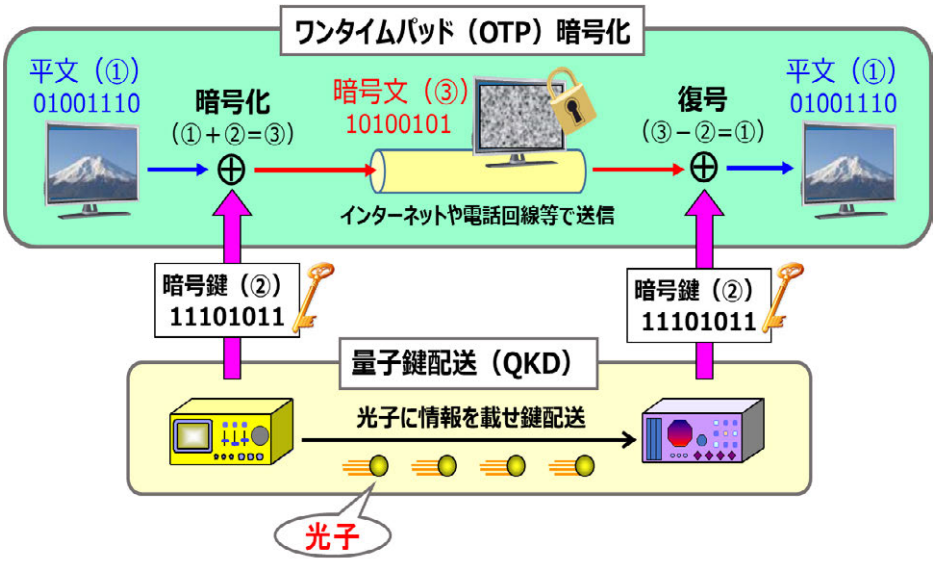


図 1　量子暗号の仕組み

【何に／何故必要か】

現在普及している暗号は、解読に膨大な計算量を必要とする「計算量的安全性」により秘匿性が担保されていますが、将来、量子コンピュータや全く新規の計算技術・数理アルゴリズムの出現により、解読が容易になってしまう潜在的脅威があります。特に何十年にわたる秘匿性が要求される重要情報の場合、悪意のある第三者は、現在は解読する技術を持たなくてもとりあえず暗号化データを盗聴・入手し、将来新しい計算技術を確立してから解読する、いわゆる「harvest now, decrypt later」攻撃を仕掛けることが可能です。

一方、量子暗号は、いかなる計算機でも将来にわたり原理的に解読不可能な情報理論的安全性を持ちます。情報理論的安全性を実現できる暗号技術は、現状量子暗号のみです。その意味で、現在知られている暗号技術の中で最も強力な秘匿性を実現することができます。安全保障をはじめとする国家機密の保護や、医療、金融、インフラ、スマート製造などの分野で、超長期秘匿性が要求される情報を守ることができます。

【国内外現状】

日本を始め、欧米中韓などの各国で研究開発、社会実証が進み、国際標準化や本格的な実用化が始まりつつあります。

【必要となるであろう要求条件】

多数の QKD 送受信機をネットワーク接続し、安全かつ効率的に運用する QKD ネットワーク技術の確立が必要です。QKD ネットワークでネットワーク上の任意の 2 地点（または複数地点）で暗号鍵を共有し、これを従来のネットワーク（古典ネットワーク）に供給することで、情報理論的に安全な暗号鍵を使ったセキュリティサービスが可能になります。

01 第1章 はじめに

（4）量子ネットワーク

【どんな技術か】

古典的なデジタル情報（0, 1）ではなく、量子情報（量子コンピュータで使われる量子ビットや、量子的な相関を保持した量子もつれ状態など）をネットワーク上に配信し、様々な応用に利活用するための通信基盤が量子ネットワークです。

【何ができるのか】

量子情報を直接配信できると、現在実現しているよりも長距離の量子暗号や、離れて配置する光時計（精密光信号を発生する原子時計）を接続して、従来技術では不可能な正確性で時間を刻む光時計量子ネットワークが実現できると期待されています。また、複数の小・中規模の量子コンピュータを量子ネットワークに接続することで高い演算能力を有する大規模量子コンピュータの構築が可能になります（分散量子コンピューティング）。さらに、遠隔にある大型量子コンピュータを量子ネットワークに接続することで、計算内容を誰にも知られることなく量子計算を実行できる秘匿量子計算が可能になると期待されています。

【国内外動向】

要素技術となる量子物理の基礎研究は世界中で進められてきました。欧米では 2020 年前後から動作原理のフィールド実証に向けた取り組みが開始され、日本でもテストベッド構築に向けた検討が始まっています。

【必要となるであろう要求条件】

量子情報を保存・処理する量子メモリ技術、光信号と量子メモリの間をつなぐ量子インターフェース技術、量子情報（特に量子もつれ）を壊さずに中継伝送する量子中継技術などの要素技術が必要です。これらは、まだいずれも基礎研究段階であり、様々な物質材料や中継方式の候補があり、試行錯誤が行われている段階です。

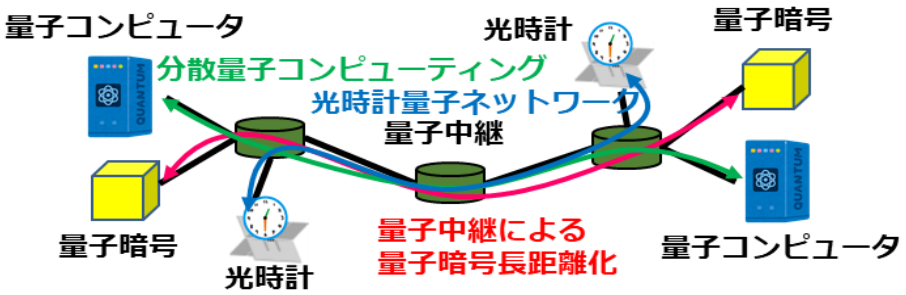


図 2　量子ネットワークの仕組み

（5）量子インターネット

「量子インターネット」の定義について、米国や欧州の量子技術の研究戦略や研究プロジェクトなどでは下表のようにまとめられています。

「量子インターネット」は、量子コンピュータや量子センサなどの量子情報機器・デバイスが接続されたグローバルな量子ネットワーク、といえます。また、現在のインターネットが、複数のネッ

01 第1章 はじめに

トワークが相互に接続され、デジタル情報（bit）が流通するネットワークであることを踏まえると、「量子インターネット」は、複数の「量子」ネットワークが相互に接続され、「量子情報（qubit）」が流通するネットワークになるとも考えられます。

今後、国際的な学会等で議論が行われ、「量子インターネット」の要素技術が成熟していく過程で「量子インターネット」の定義が明確になると考えられます。

インターネットが登場した頃は、現在のようにインターネットが社会経済活動や人々の生活に不可欠な基盤となることを誰も想像していませんでした。「量子インターネット」が、どのようなネットワークになるか、どのような使い方がされるのか現時点でははっきりしませんが、将来、現在では考えられない未来のアプリケーションやサービスが「量子インターネット」上で提供され、人々の生活をより豊かに安全・安心にすることが期待されます。

表１　量子インターネットの定義例

組織・文書		定義例
米国	”A STRATEGIC VISION FOR AMERICA'S QUANTUM NETWORKS”（2020.2）, National Quantum Coordination Office, White House	The quantum internet—a vast network of quantum computers and other quantum devices.
	“Quantum Internet Blueprint Workshop” (2020.10), Department of Energy（DOE）	The international research community perceives the construction of a first prototype global quantum network—the Quantum Internet—to be within reach over the next decade.
欧州	Quantum Internet Alliance(QIA)	The long-term ambition of the European Quantum Internet Alliance is to build a Quantum Internet that enables quantum communication applications between any two points on Earth.
	“Strategic Research Agenda on Quantum Technology”(2020.3), Quantum Flagship Project	“Quantum Internet”: quantum computers, simulators and sensors interconnected via quantum networks distributing information and quantum resources such as coherence and entanglement to secure our digital infrastructure.
標準化団体	IRTF (Internet Research Task Force)	Quantum Internet - A network of Quantum Networks. The Quantum Internet will be merged into the Classical Internet to form a new Hybrid Internet. The Quantum Internet may either improve classical applications or may enable new quantum applications.

02 第2章 量子ネットワークが実現する社会像・ユースケース

1．量子ネットワークが実現する社会像

（1）全体像

量子ネットワークが実現する社会像として、年代ごとに実現が想定されるユースケースをまとめました。

2020 年代は、QKD ネットワークにより、医療・製造・金融分野などで重要な情報のセキュアなやり取りが実現することが期待されます。

2030 年代以降は、QKD ネットワークの広域化により、さらに多様な分野で安心・安全な情報の流通が可能となることが期待されます。また、量子コンピュータや量子センサが接続された量子ネットワークの社会への展開が始まります。

2040 年代には、複数の量子ネットワークがグローバルに相互に接続された「量子インターネット」が構築され、これまでにはない新しいアプリケーションやサービスが登場し、「量子インターネット」が人々の豊かな生活や社会経済活動を支える基盤となることが期待されます。

表２　量子ネットワークのユースケース（全体像）

	ユースケース例	量子ネットワーク技術の進展	量子コンピューティング・量子センシング技術の進展
2020 年代	●医療：電子カルテやゲノム情報など、漏洩することで生涯にわたって影響がある生体情報のやり取り ●製造：企業の営業秘密・ノウハウ、重要技術など、漏洩することで企業活動に大きな影響がある情報のやり取り ●金融：金融システム等に係る情報などのやり取り	・QKD（関東圏→全国規模）	・NISQ 量子コンピュータ IBM[1] 2020 年：65qubit 2021 年：127qubit 2022 年：433qubit 2023 年：1121qubit
2030 年代	●行政・外交・安全保障：行政における個人情報のやり取り、在外公館における機密情報の通信、機密情報のやり取り ●生活：モバイル端末向け暗号自動販売機などの活用による家庭レベルでの超セキュアインターネット（個人の医療情報・金融情報などのやり取り）	・QKD（全国規模→グローバル規模） ・衛星 QKD/ 物理レイヤ暗号 ・量子ネットワーク	・NISQ 量子コンピュータ ・小規模エラー耐性量子コンピュータ ・量子センサ
2040 年代	★化学・材料・創薬など：量子ネットワークに接続された量子コンピュータによる新素材・新薬等の発見 ▲防災・災害対応：量子ネットワークに接続された量子センサーによる微弱な重力変動などの監視 ●資源開発：月・火星における掘削ロボットの大容量画像伝送（シャノン限界越え量子符号化）	・QKD（グローバル規模） ・衛星量子通信 ・量子ネットワーク（グローバル規模）	・エラー耐性量子コンピュータ ・分散量子コンピューティング ・量子センサ

●：QKD、★：量子コンピュータ、▲：量子センシングによるユースケース例

1　https://www.ibm.com/blogs/think/jp-ja/ibm-quantum-roadmap/

02 第2章 量子ネットワークが実現する社会像・ユースケース

2. 量子鍵配送 (QKD) ネットワークにより実現する社会像・ユースケース

（1）QKD ネットワークにより守るべき情報

漏洩すると重大な影響がある安全保障、外交、防衛、個人のゲノム情報などは長期にわたって守る必要があります。これらの情報をネットワークにより共有する際には、情報理論的安全性が担保された QKD の活用が期待されます。

表３　QKD により守るべき情報の例

情報保有者	守るべき情報の例
国・自治体	・外交関連情報、防衛関連情報、安全保障情報、地理情報（インフラ、地下空洞）、戸籍・住民情報、選挙の投票情報　など
組織（企業等）	・顧客名簿、新規事業計画、価格情報、対応マニュアル（営業情報） ・新規技術、製造方法・ノウハウ、設計図面等（技術情報）　など
個人	・健康情報、ゲノム情報、思想・信条・嗜好、暗証番号、クレジットカード番号、パスワード　など

（2）QKD により実現する社会像・ユースケース

QKD の実用化により、医療・産業・サービス・行政・外交・安全保障・生活などにおいて、情報理論的に安全な通信が実現します。

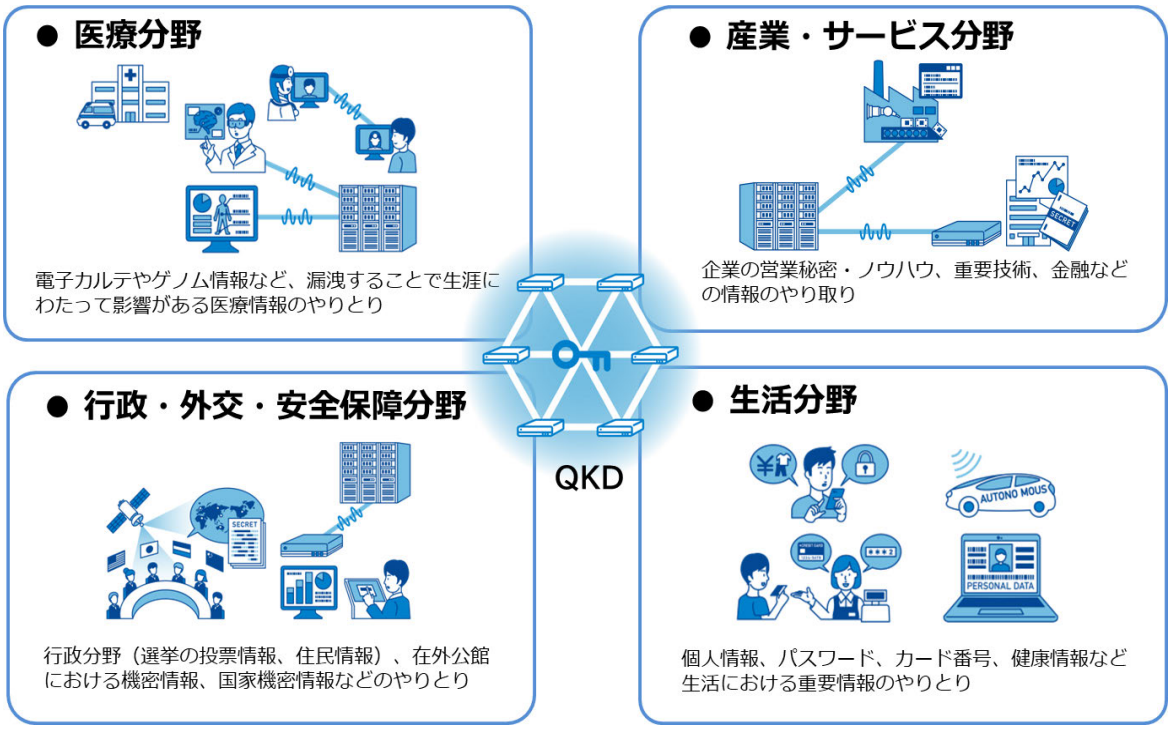


図３　QKD により実現するユースケース例

02 第2章 量子ネットワークが実現する社会像・ユースケース

（3）個別分野のユースケース事例

①医療・金融分野～量子セキュアクラウドによる安全なデータ流通／保管／利活用～

【背景・必要性】

企業の重要な経営資源の一つである大容量の情報を暗号化などにより安全に保管し、必要に応じて完全に復元することは重要な課題です。現時点では、現在普及している暗号技術によって安全に通信を行うことができていますが、量子コンピュータの高度化により、電子決済、個人情報のやりとり等で使われる高秘匿情報通信に用いられる暗号が解読される恐れがあり、決して破られない暗号技術が求められます。

【技術概要】

量子セキュアクラウド技術は、量子暗号技術と秘密分散技術、耐量子計算機暗号技術等を融合し、データの安全な流通／保管／利活用を可能とするクラウド技術です。QKD ネットワークと秘密分散により、情報理論的に安全なデータの保管・交換を実現します。また、ネットワーク上のユーザ認証や改ざん防止の署名発行には、量子コンピュータでも解読に膨大な計算量を必要とすると言われる耐量子計算機暗号をベースとした認証基盤（耐量子－公開鍵認証基盤）を活用します。

量子セキュアクラウド技術の確立により、改ざん・解読が不可能な高いセキュリティ性を担保するだけでなく、例えば、医療、新素材、製造、金融分野で蓄積された個人情報や企業情報など秘匿性の高いデータの収集／分析／処理／利用を可能とします。

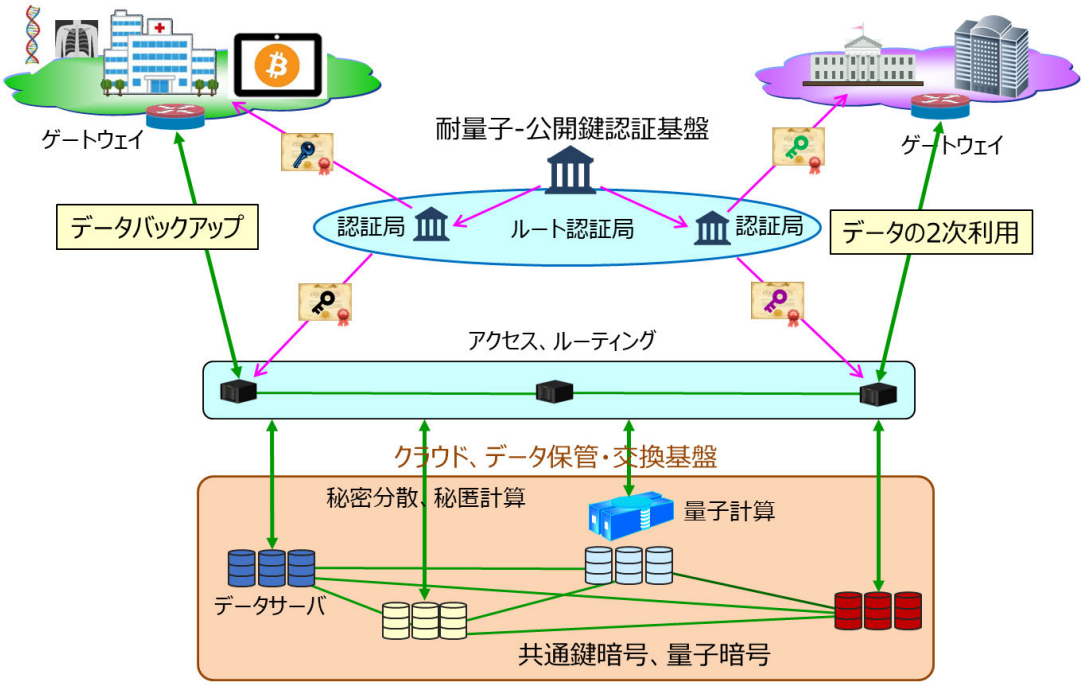


図４　量子セキュアクラウド技術の仕組み

02 第2章 量子ネットワークが実現する社会像・ユースケース

②行政・外交・安全保障分野～衛星 QKD による安全な基幹ネットワーク～

【背景・必要性】

国の安全保障・機密に関わる情報や、自治体における個人の情報を、都市間や国家間のように広域にまたがる拠点間で安心してやり取りするためには、QKD ネットワークが日本国内や大陸間に張り巡らされていることが必要です。

しかし、QKD は原理的に信号の減衰に弱く、光ファイバによる量子暗号の長距離伝送は困難なものになります。そのため、広域な QKD ネットワークの実現には、光ファイバよりも信号の減衰が少ない宇宙空間を使った、衛星による量子暗号通信ネットワークが重要になります。

【技術概要】

この衛星 QKD による基幹ネットワークでは、静止軌道衛星と地上とのリンクに加えて、低軌道・中軌道における複数衛星（コンステレーション衛星）の活用や、地上 QKD ネットワークとの連携により、堅牢性・可用性を高めます。

将来的には、月や火星との間の量子通信リンクを確立することで、探査・開発のためのインフラとしての役割を果たすことも期待されます。

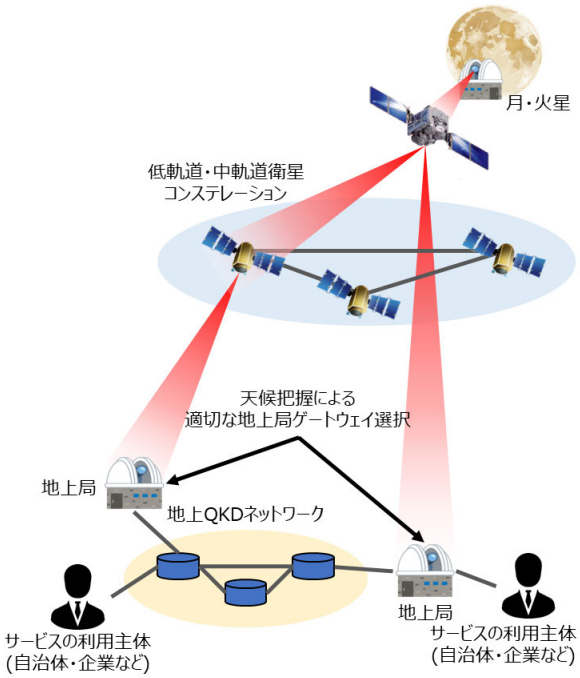


図５　衛星 QKD による安全な基幹ネットワーク

③産業・サービス分野～光空間通信によるローカル秘匿ネットワーク～

【背景・必要性】

企業等が長年をかけて積み重ねてきた営業秘密、ノウハウ、技術情報などは、産業・サービス分野における重要な情報です。これらの情報を産業スパイなどによる情報漏えいから守る一つの方法が、企業等が敷地・オフィスビル内や主要支社間といったスケールで独自に展開可能な、光空間通信によるローカル秘匿ネットワークです。

02 第2章 量子ネットワークが実現する社会像・ユースケース

【技術概要】

企業等が独自に敷設可能な秘匿ネットワークには、①外部機関と独立に構築できること、②安価に構築できること、が求められます。QKD の中でも、現行の光通信で用いられている装置や構成部品で低価格に実現可能と期待される方式である CV-QKD（Continuous-Variable QKD: 連続量－量子鍵配送）を光空間通信で実施することにより、新たに光ファイバを調達・敷設せずとも、上記の要件を満足する秘匿ネットワークを構築できます。また、電波と比較して、光は空間的な広がりが小さいため、第 3 者の盗聴が困難であるという光空間通信特有の性質を活用した秘匿通信（物理レイヤ暗号通信）（第 4 章参照）と組み合わせることで、様々なユーザ要件にも対応可能なネットワークを構築できます。

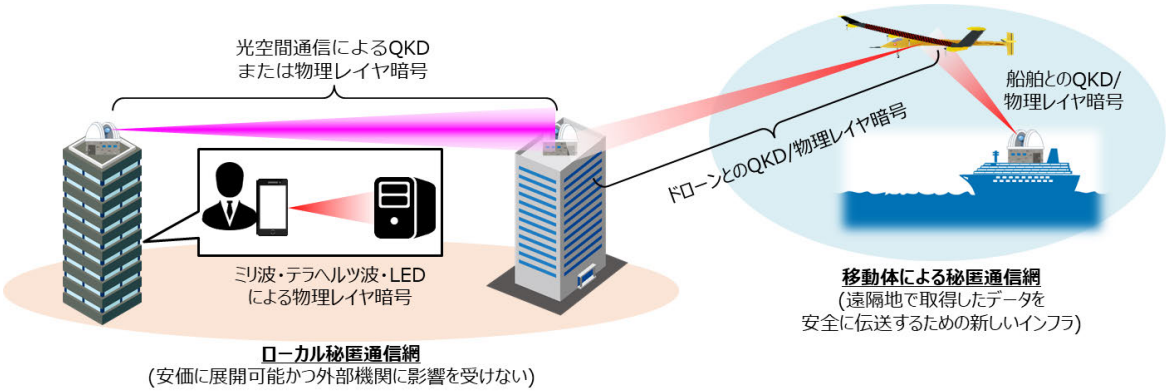


図６　QKD や物理レイヤ暗号によるローカル秘匿ネットワーク

④生活分野～誰でも利用可能な高セキュリティ基盤～

【背景・必要性】

5G 技術の発達により、モバイル端末を介したサービスが生活に浸透してくると、パスワード、カード番号、健康情報など生活における重要情報の漏えい、さらには家電などの遠隔制御機器の乗っ取りといった個人レベルのセキュリティリスクが表面化します。個人レベルのセキュリティを確保するには、セキュリティを提供する事業者のような組織と個人の間で非対称な関係が生じないよう従来以上の配慮が要求されます。

そのため、現行のセキュリティ基盤で用いられている安全性技術をアップデートした、新しいセキュリティ基盤が必要となります。

【技術概要】

この基盤では、通常のネットワーク（古典ネットワーク）上の鍵交換や認証が量子コンピュータでも解読困難な暗号技術（耐量子計算機暗号）で行われます。さらに、モバイル端末とアクセスポイントとの間の通信を物理レイヤ暗号で行うことで、ネットワークの安全性をより高めることができます。これらの技術はモバイル端末にもアルゴリズムとして実装可能であるため、個人が莫大な負担を強いられることなく、この基盤を利用することができます。

02 第2章 量子ネットワークが実現する社会像・ユースケース

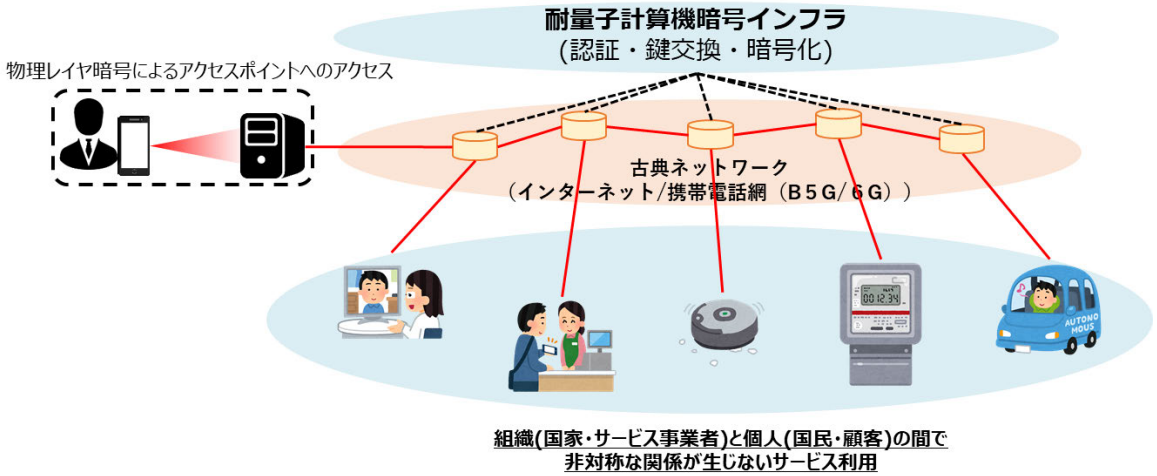


図7　耐量子計算機暗号インフラによる新たなセキュリティ基盤

3．量子ネットワークにより実現する社会像・ユースケース

（1）社会像・ユースケース

量子ネットワーク（量子インターネット）が実現することにより、人々の安心・安全・便利な生活や高度な社会経済活動が実現することが期待されます。

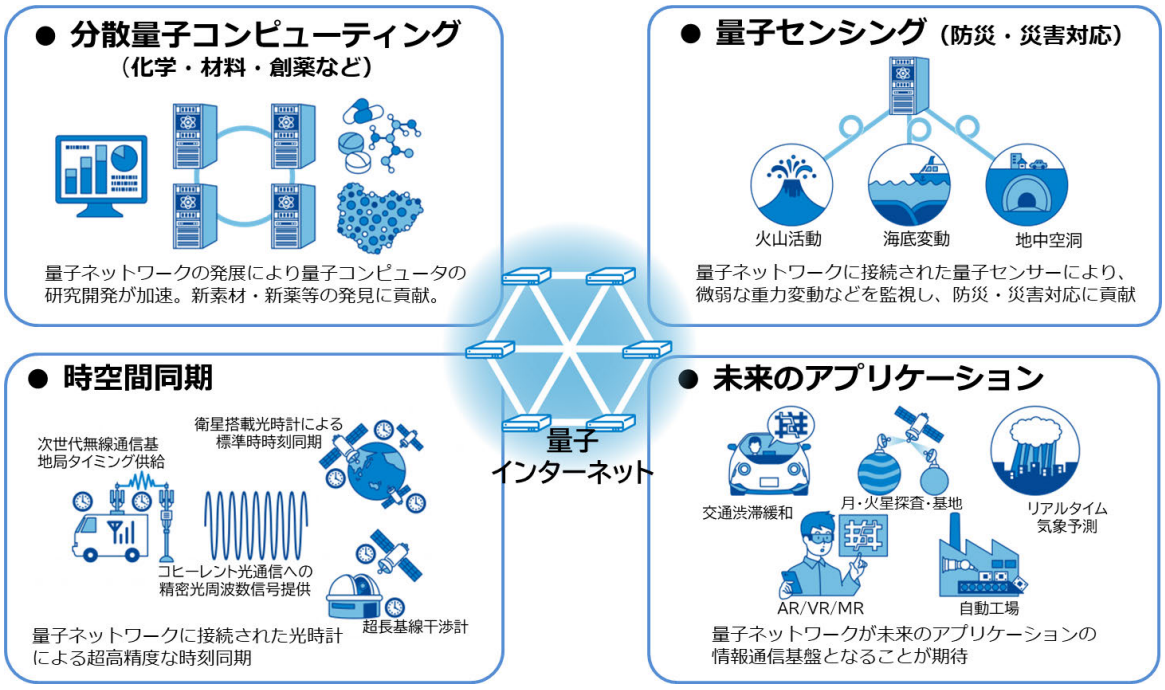


図8　量子ネットワークにより実現する社会像・ユースケース

02 第2章 量子ネットワークが実現する社会像・ユースケース

（2）個別分野のユースケース事例

①量子センシング～防災・災害対応など～

【背景・必要性】

高精度タイミング供給と局所重力センシングが可能な光時計（量子センサの一つ）を量子ネットワークに接続し、検知した地震、火山噴火、地滑りなどの重力場変動の情報を量子ネットワークを使って送ることで、従来よりも早期に災害警報を出すことなどが可能となります。

また、高精度な時空間同期を実現することにより、次世代の通信システムや新しいタイムビジネスの登場が期待されます。

【技術概要】

光時計が検知した重力場変動などの情報を量子ネットワークを使って送るためにはコヒーレントリンクという技術が必要です。コヒーレントリンクは光時計の生成する光周波数を光の波として接続して光時計の時刻の比較や同期を行う技術です。光時計の量子ネットワークは、光時計が生成する精密光周波数をコヒーレントリンクに付加することにより物理学で許される最速の測定を実現できます。

また、コヒーレントリンクに加えて、量子ゲート操作が可能な光時計、光子との量子インターフェース、二光子干渉測定技術などの要素技術が必要となります。

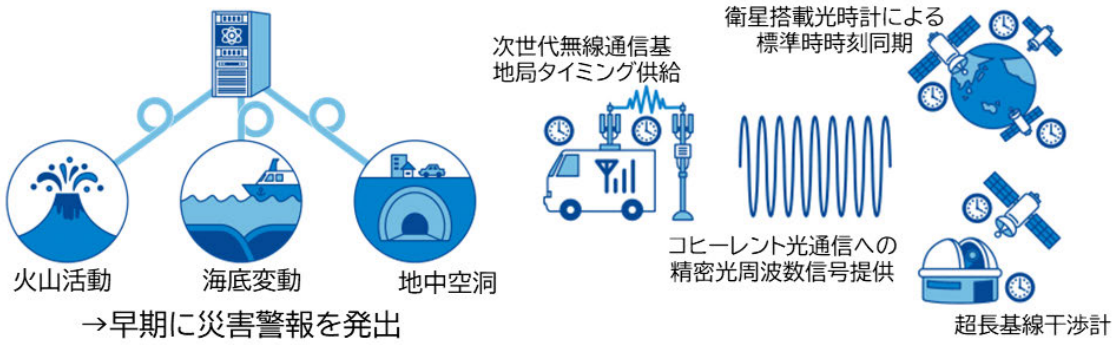


図９　光時計の量子ネットワークのユースケース

（2）個別分野のユースケース事例

②分散量子コンピューティング～化学・材料・創薬など～

【背景・必要性】

量子コンピュータによって、これまでのスーパーコンピュータなどでは困難であった、超大規模な分子構造のシミュレーションなどが可能となり、新薬や新しい性能を持つ材料の創出や未来の社会基盤となる新しいユースケースの登場などが期待されます。

さらに、量子コンピュータが量子ネットワークにより接続されることによって、より大規模な計算や量子コンピュータの開発の加速などが可能となると期待されます。

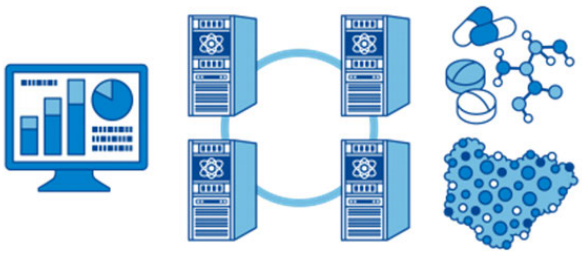
このような大規模な量子コンピュータによる計算は、クラウドサービスでの提供が想定されるため、計算内容を秘匿したまま、量子計算を行うことができるような方法が求められます。量子ネットワークで大規模量子コンピュータに接続した小規模量子コンピュータを用いることで、このようなブラインド量子計算が可能になると期待されます。

02 第2章 量子ネットワークが実現する社会像・ユースケース

【技術概要】

量子コンピューティングは、古典的なデジタルビット（0,1）に代わり、量子物理学に基づく量子ビット（qubit）を用いることで、量子ビット数に対して指数的に増大する計算リソース（「ヒルベルト空間」と呼ばれます）である種の計算問題を高速に解決する計算手法です。分散量子コンピューティングは、量子コンピュータを量子ネットワークで接続して、全体で量子コンピューティングを拡張する手法です。

量子コンピュータを量子ネットワークで量子ビットレベルでの接続を行うために、多岐にわたる技術が必要となります。量子ネットワークに関しては、量子もつれ状態を光ファイバで共有するための、量子中継器、量子ネットワーク技術や、小・中規模量子コンピュータの構築技術などの研究開発が必要です。



量子ネットワークの発展により量子コンピュータの
研究開発が加速。新素材・新薬等の発見に貢献。

図 10　分散量子コンピュータネットワークのユースケース

03 第3章 量子ネットワークの進展イメージ

第 3 章では、量子ネットワークの進展イメージを、2025 年代、2030 年代、2040 年代の年代別にまとめています。

技術の普及・進展により、QKD ネットワークや量子中継を使った量子ネットワークが段階的に導入されていきますが、現在のインターネット／携帯電話網などのネットワーク（古典ネットワーク）が量子ネットワークに置き換わるわけではなく、古典ネットワークと量子ネットワークが共存することで、前章で示した様々なサービスが実現可能になります。以下、その段階的な普及イメージを概観します。

1．2025 年頃のイメージ

地上・衛星を相互に接続した QKD ネットワークのサービス運用が開始され、セキュアな通信サービスが開始することが想定されます。また、古典ネットワークを使った量子コンピューティング、量子計測・センシングを用いたサービスが開始することが想定されます。

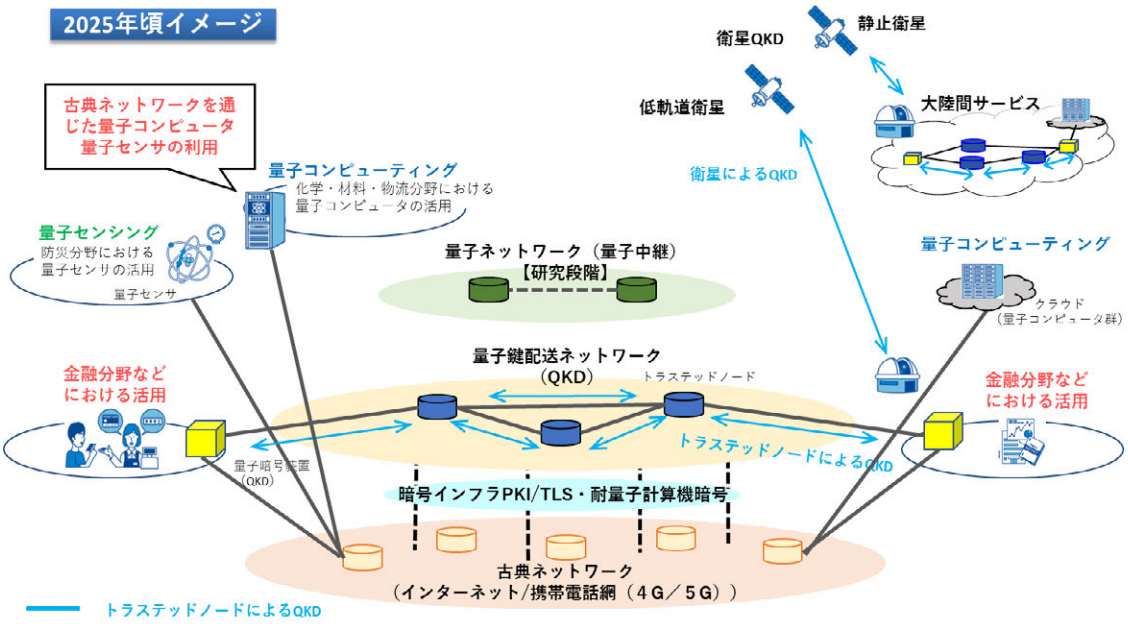


図 11　2025 年頃の量子ネットワークの進展イメージ[2]

2．2030 年頃のイメージ

地上・衛星を相互に接続した QKD ネットワークのサービス運用が開始され、セキュアな通信サービスが拡大することが想定されます。また、古典ネットワークを使った量子コンピューティング、量子計測・センシングを用いたサービスが拡大することが想定されます。

2　図中略語　PKI（Public Key Infrastructure）：公開鍵基盤、TLS（Transport Layer Security）：インターネット上の通信においてセキュアな通信路を確保する仕組み。

03 第3章 量子ネットワークの進展イメージ

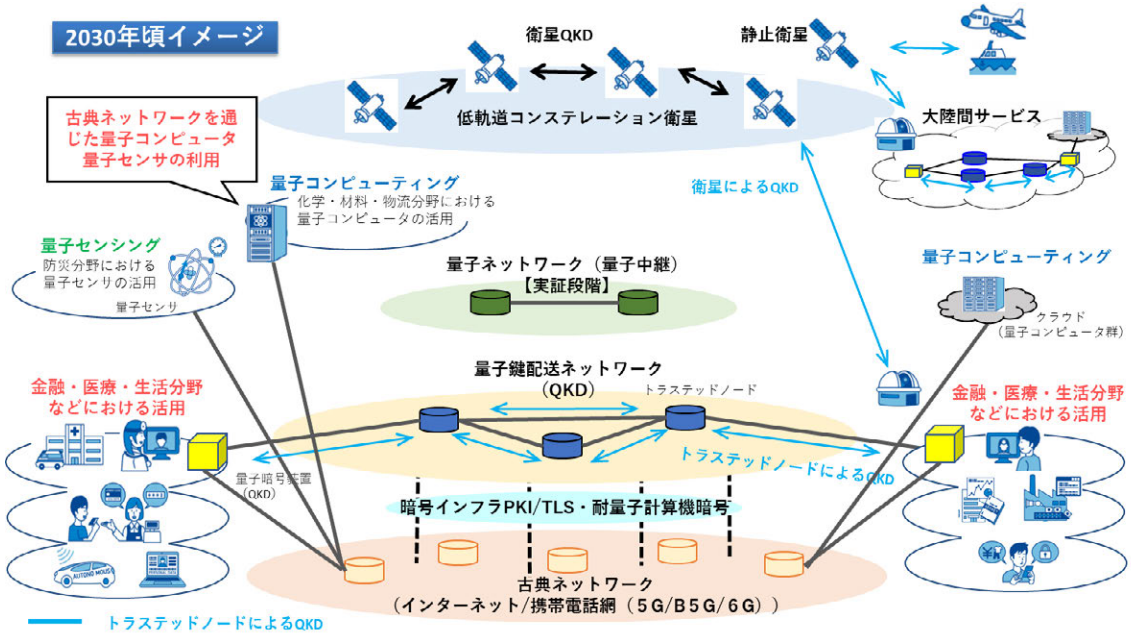


図 12　2030 年頃の量子ネットワークの進展イメージ

3．2040 年頃のイメージ

衛星・地上のグローバルな量子ネットワークが構築され、多種類の量子ネットワーク／プロトコルを収容する仮想量子ネットワークサービスが実現することが想定されます。

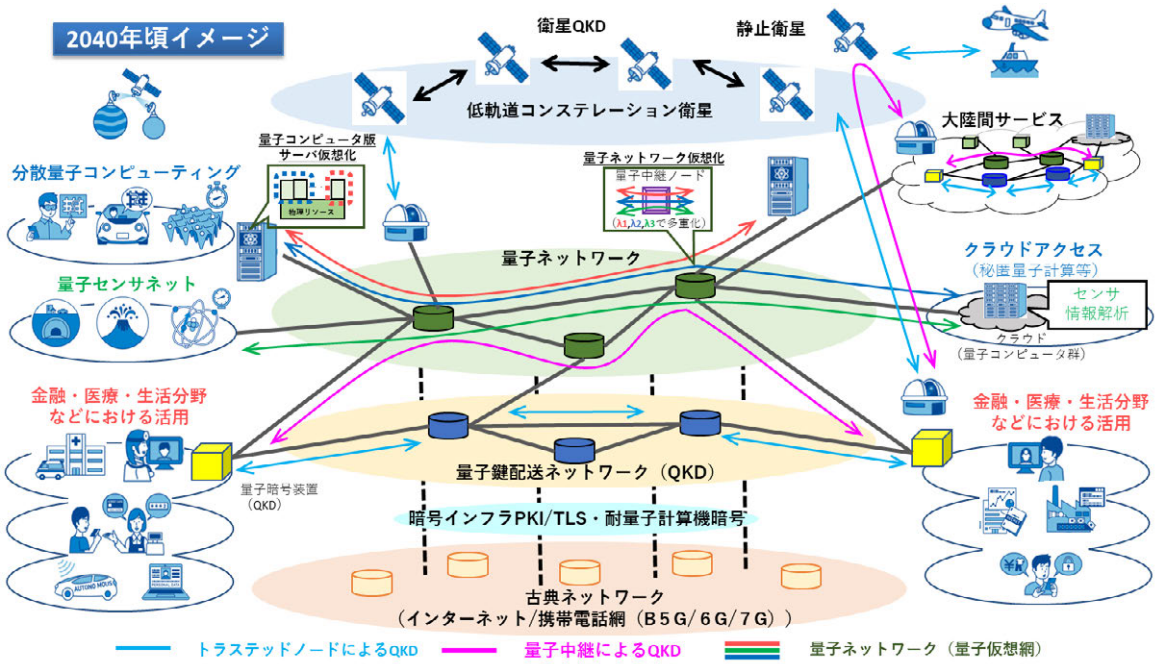


図 13　2040 年頃の量子ネットワークの進展イメージ

03 第3章 量子ネットワークの進展イメージ

また、2040 年頃の量子ネットワークのサービスイメージについて、量子ネットワークを使ったアプリケーション／コンテンツ事業者の要求に応じて、インフラ事業者や量子仮想ネットワークオペレータ（Virtual Network Operator: VNO）が仮想量子ネットワークを構築し、サービスを提供することが想定されます。

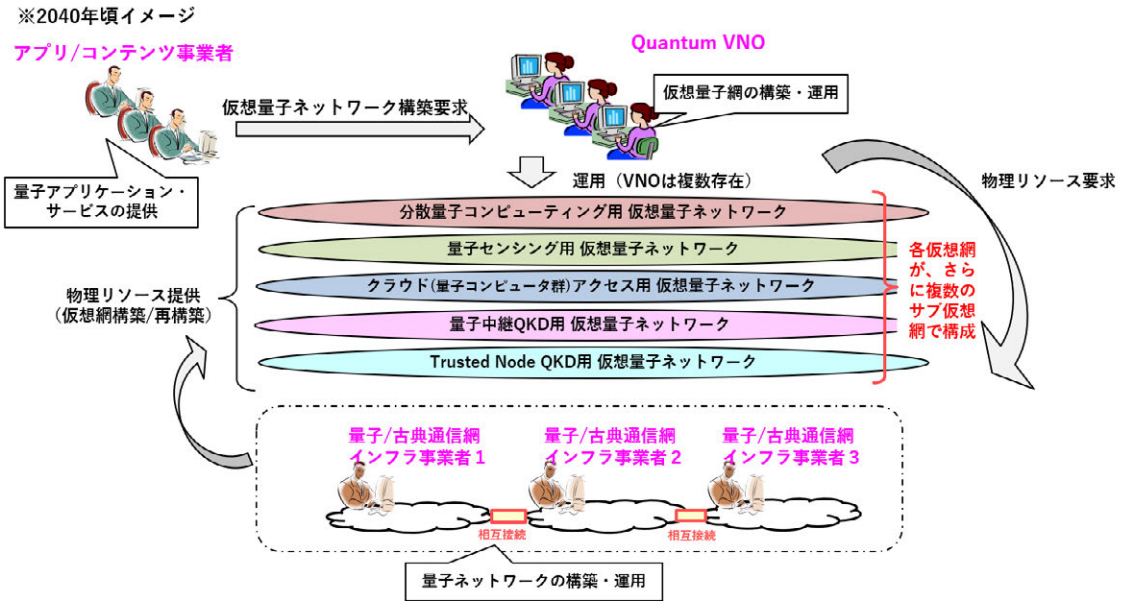


図 14　2040 年頃の量子ネットワークのサービスのイメージ

04 第4章 要素技術と要求条件

1．量子ネットワーク技術の全体像

（1）技術課題の全体像

下図は「量子技術イノベーション戦略」（2020 年 1 月）における量子ネットワークの技術課題を示しています。このうち、NICT は下図の赤字に該当する技術の研究開発を進めています。

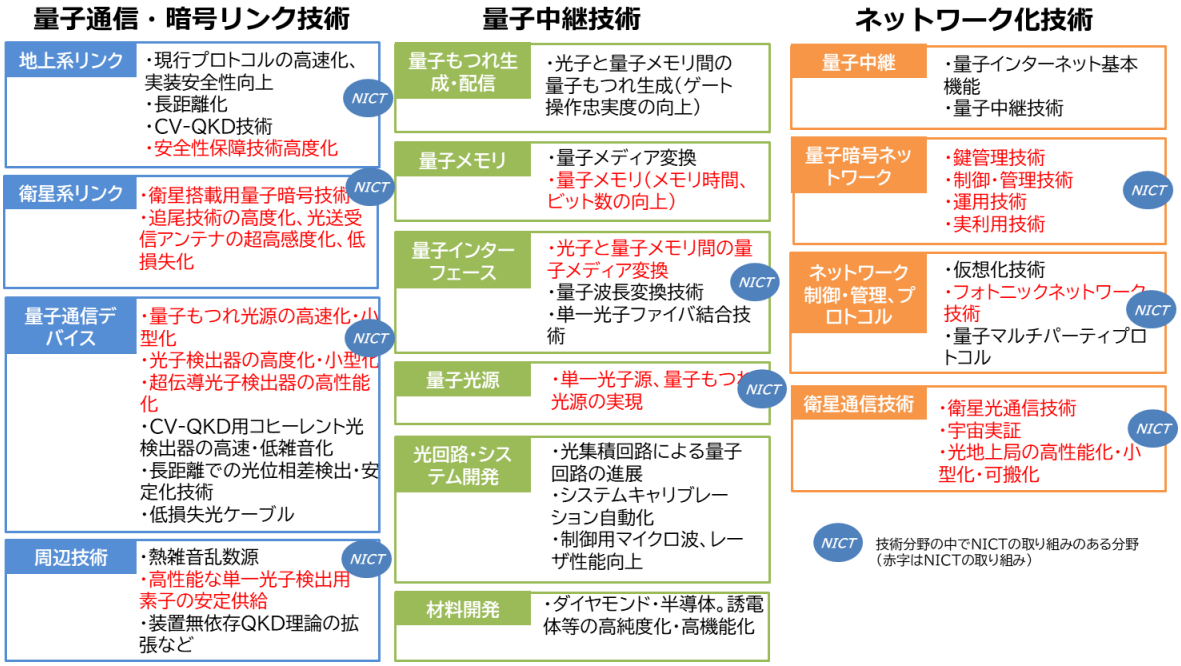


図 15　量子ネットワーク技術の全体像

（2）NICT における取り組み

NICT では、QKD ネットワーク、衛星・空間通信、量子ネットワークに関する研究開発を進めています。次項ではこれらの要素技術と要求条件の概要を説明します。

（1）量子鍵配送（QKD）ネットワーク	（3）量子ネットワーク
①量子鍵配送(QKD)	①量子インターフェース
②鍵管理・鍵リレー技術	②量子中継
③QKDネットワーク制御・管理技術	③多種量子ネットワーク制御管理
④量子セキュアクラウド技術	④量子センサネットワーク（光時計量子ネットワーク）
（2）衛星・空間通信	⑤量子コンピューティング（イオントラップ量子コンピュータ）
①衛星量子鍵配送(QKD)技術	⑥量子コンピューティング（超伝導量子コンピュータ）
②物理レイヤ暗号技術	
③衛星ー地上ネットワーク連携技術	

図 16　NICT における量子ネットワーク技術の研究開発の取組（全体像）

04 第4章 要素技術と要求条件

2．要素技術と要求条件

（1）量子鍵配送（QKD）ネットワーク

【概要】

QKD をネットワーク化し、ネットワークの任意の 2 地点（または複数地点）に暗号鍵を提供することを可能にする技術です。QKD ネットワークで共有された暗号鍵は、通常のネットワークに提供され、その上で動くアプリケーションでの暗号化通信に使われます。つまり QKD ネットワークを従来のネットワークにアドオンすることで、これまでにない超長期安全な暗号鍵の提供が可能になる技術です。QKD ネットワークの応用の 1 つが量子セキュアクラウド技術です。

【必要な要素技術】

QKD 装置（QKD を行う送受信機。QKD モジュールとも呼ばれる）の他、後述の鍵管理・鍵リレー、QKD ネットワーク制御・管理などの要素技術が必要です。また、ノードの安全性の確立（トラステッドノード）が必要になります。

【国内外動向】

日欧米中韓などで実証実験・試験運用が進んでいます。日本が 2010 年に構築したテストベッド「東京 QKD ネットワーク」は、世界最長期間の運用実績を有しています。QKD 装置については ID Quantique（スイス）、Quantum CTek（中）、東芝（日）などが製品化と運用サービスを始め、NEC（日）もフィールド試験段階に入っているほか、各国で多数のスタートアップが開発を進めています。また、QKD ネットワークサービスも CAS Quantum Network（中）、Quantum Xchange(米) などが事業化を進めているほか、BT（英）、Verizon（米）、SK Telecom（韓）などの既存通信企業も参入しつつあります。

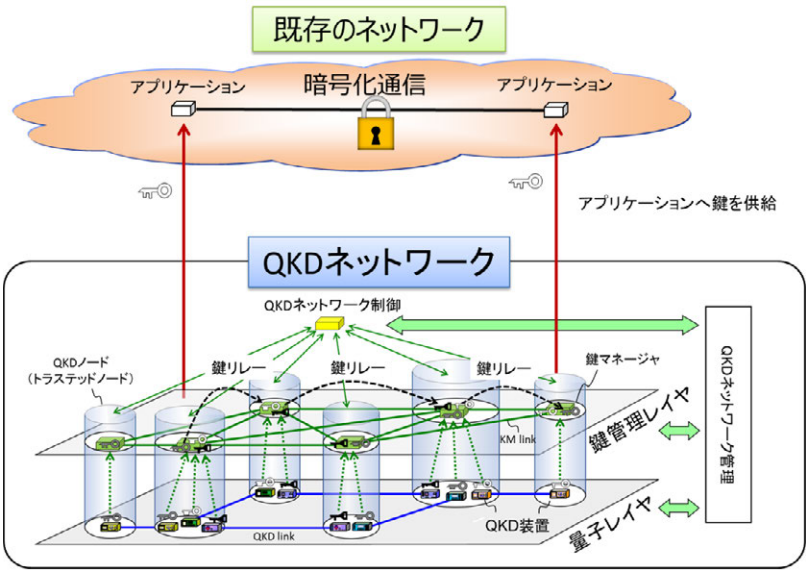


図 17　QKD ネットワークの構成

04 第4章 要素技術と要求条件

【参考】QKD ネットワーク技術の国際標準化

NICT は、政府や企業等と連携し、QKD ネットワーク技術のグローバルな普及に向けて、国際電気通信連合電気通信標準化部門（ITU-T）や国際標準化機構・国際電気標準会議第一合同技術委員会（ISO ／ IEC）において国際標準化を積極的に推進しています。

ITU-T では、2019 年 10 月に量子暗号分野における初の国際標準勧告 ITU-T Y.3800「Overview on Networks Supporting Quantum Key Distribution」が、東京 QKD ネットワークの基本仕様を採用する形で発刊されました。本勧告を皮切りに、ITU-T では現在 10 篇を超える勧告の発刊・開発が進み、日本も主導的に関わっています。

ISO ／ IEC JTC 1 では、QKD 装置の安全性評価に関する標準化の策定に積極的に参加しています。QKD 装置はセキュリティデバイスであるため、これを適切に市場に流通させるためには、安全性や運用に関するガイドラインや、製品化された QKD 装置が安全性の観点から正しく実装・運用されていることを保証するための評価・検定・認証制度の整備が必要になります。

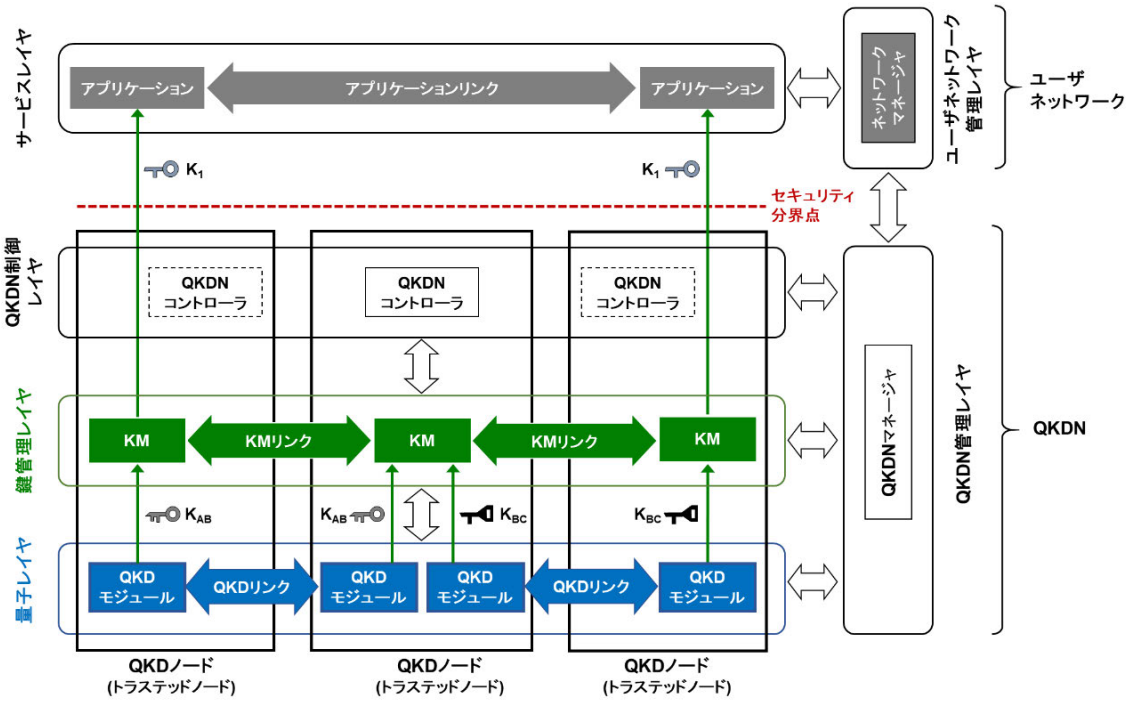


図 18　ITU-T Y.3800 で規定された QKD ネットワークの基本構成[3]

以下、QKD ネットワークに必要な要素技術、及び応用である量子セキュアクラウド技術について説明します。

①量子鍵配送 (QKD)

【どんな技術か】

光の粒である光子を使って離れた 2 者間で暗号鍵を共有する技術です。量子力学の「不確定性原理」という性質により、光子へのいかなる盗聴攻撃でも確実に検知し、盗聴の恐れの無い鍵情報のみを暗号鍵とすることにより、情報理論的に安全な暗号鍵の生成を可能にします。一方、光子は極めて弱い信号であり、また通常の光通信の中継増幅器は光子の量子状態を壊してしまうため使えないことから、一対の QKD 送受信機で鍵生成できる距離は現状、長くても 50 ～ 100km 程度に制限されます。

3　図中略語　QKDN: QKD Network（QKD ネットワーク）、KM: Key Manager（鍵マネージャ）

04 第4章 要素技術と要求条件

②鍵管理・鍵リレー技術

【どんな技術か】

鍵管理は、QKD により生成された鍵を安全に管理し、適切にアプリケーションに供給する技術です。鍵リレーは、QKD で生成された鍵を別の QKD により作られた暗号鍵と OTP 暗号化により、離れたノードまで安全に伝送する技術で、安全性の保証されたノード（トラステッドノード）と組み合わせることで、単体の QKD 送受信機だけでは不可能な長距離間での鍵生成や QKD のネットワーク化を可能にします。

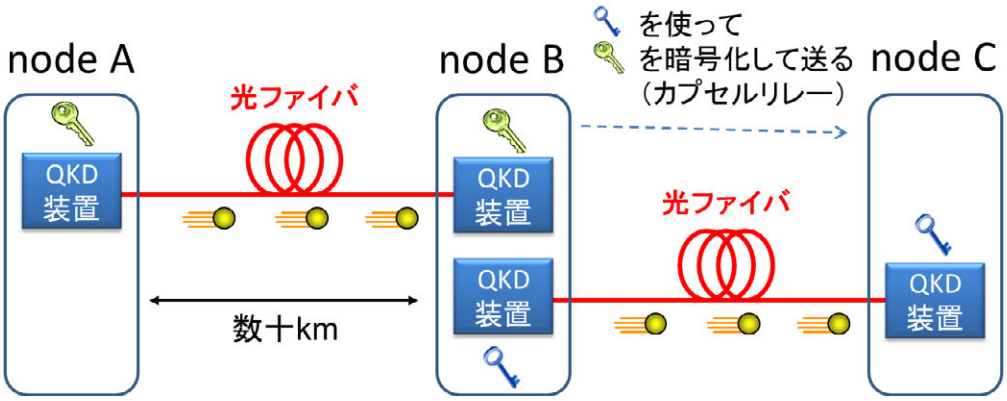


図 19　量子鍵リレーの仕組み

③ QKD ネットワーク制御・管理技術

【どんな技術か】

QKD ネットワーク制御技術は、QKD ネットワークにおいて送受信間のセッション制御、アクセス制御、鍵リレーの経路制御及び経路切替、ポリシー制御、ネットワーク構成の制御などを行う技術です。QKD ネットワーク管理技術は、QKD ネットワークの各要素やリンクの状況等を監視しネットワーク全体を適切に管理するための技術です。ネットワーク仮想化 / 自動化技術や情報指向型通信技術を始め、従来のネットワーク制御・管理技術が様々に応用できると考えられており、ユーザが必要な時に必要なサイズ及びセキュリティレベルの暗号鍵を効率的に配信できるようになります。

④量子セキュアクラウド技術

【どんな技術か】

量子暗号、秘密分散、耐量子－公開鍵認証基盤、秘匿計算等を融合することにより、どんな計算機でも解読や改竄のできないデータバックアップ保管と計算処理を実現する技術です。複数のデータサーバを量子暗号による秘匿回線で結びストレージネットワークを構成し、その上に秘密分散アルゴリズムを実装して、原本データの情報理論的に安全なバックアップ保管を実現します。

一部のデータサーバから情報を盗み出しても元のデータの復元が不可能であるという秘匿性と、逆に一部のデータサーバが災害等で失われてもユーザは残りのデータサーバから分散データを集め元のデータを復元できるという可用性を兼ね備えています。また、無意味化された分

04 第4章 要素技術と要求条件

散データのまま計算処理することにより秘匿計算を実現できるため、安全なデータの 2 次利用が可能になります。

ユーザ認証やデータの改ざん防止は、耐量子－公開鍵認証基盤から発行される電子署名付きの証明書を用いて行います。耐量子－公開鍵認証基盤は、今後普及してゆくと予想される次世代の暗号インフラの一つで、計算量的安全性に基づく方式です。量子セキュアクラウド上でのユーザ認証やデータの改ざん防止では、その処理を行う時間内の安全性が確保されれば十分であることから、耐量子－公開鍵認証基盤を活用しています。

このように安全性・利便性に応じた適切なセキュリティ技術を組み合わせて全体のシステムを構成します。

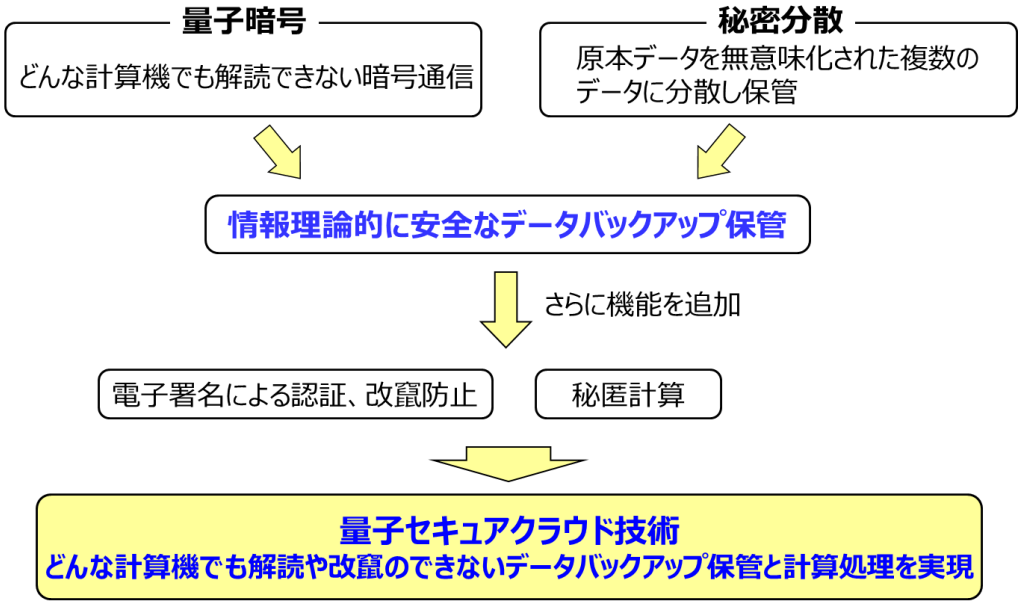


図 20　量子セキュアクラウド技術

【何に／何故必要か】

データの超長期秘匿性を確保するために必要です。例えば患者情報や遺伝子データなどの医療情報は、超長期秘匿性が求められる一方、一箇所の病院に保存するだけでは災害等によるデータ消失の懸念があり、離れた場所で安全にバックアップを取ることも喫緊の課題とされており、量子セキュアクラウドはこれらを同時に実現することができます。（量子セキュアクラウド技術の仕組み（P11）を参照）

【国内外現状】

日本の独自技術で、NICT と企業により実証実験が進んでいます。

【必要となるであろう要求条件】

QKD ネットワークと、各種の現代セキュリティ技術（秘密分散、秘匿計算、電子署名等）を適切に融合しシステム化する技術が必要です。

04 第4章 要素技術と要求条件

（2）衛星・空間通信

①衛星量子鍵配送（QKD）技術

【どんな技術か】

地上と衛星、あるいは衛星間で量子通信を実施し、情報理論的に安全な暗号鍵を共有する技術です。（衛星 QKD による安全な基幹ネットワーク（P12）を参照）

【何に／何故必要か】

地上の QKD ネットワークでは、光ファイバの伝搬損失が QKD の長距離化を阻むため、グローバル化には膨大な数の QKD 装置とトラステッドノードが必要になってきます。一方で、地球を取り巻く大気の層は 10km 程度であり、宇宙空間の損失が非常に小さいため、衛星ー地上間の通信により QKD の伝送距離を大幅に伸ばすことができます。そのため、QKD ネットワークのグローバル化には、衛星 QKD は必須の技術です。

【国内外現状】

NICT では 50kg 級の小型衛星により、QKD の基礎となる衛星 – 地上間の量子通信の実証を実施しています。[4] 一方、中国が低軌道衛星 – 地上間で QKD そのものの実験に成功するなど、[5] 現在世界各国の政府や大学、ベンチャー企業で衛星 QKD の研究加速の機運が高まっています。

【必要となるであろう要求条件】

衛星通信向けに最適化された新しい QKD プロトコルの開発に加え、衛星 – 地上間リンクを安定させるための捕捉追尾技術や補償光学技術、光子を検出するための高速・高感度な単一光子検出器技術などの開発が必要になります。

②物理レイヤ暗号技術

【どんな技術か】

「いかなる盗聴攻撃に対しても安全」な QKD と異なり、「盗聴者は送受信者の見通し外から盗聴を行う」といった、盗聴者の攻撃モデルに制限を課すことができる状況で、情報理論的に安全な暗号鍵共有を行う技術です。（衛星 QKD による安全な基幹ネットワーク（P12）、QKD や物理レイヤ暗号によるローカル秘匿ネットワーク（P12 ～ P13）、耐量子計算機暗号インフラによる新たなセキュリティ基盤（P13 ～ 14）を参照）

【何に／何故必要か】

衛星ー地上間通信やモバイル通信のように、現状の QKD では十分なパフォーマンスが出せない、あるいは実装そのものが困難であるような通信系システムにおいて、QKD の相補的な技術として用いることができます。

【国内外現状】

NICT が光空間通信での物理レイヤ暗号実証研究を行っている[6]他、QKD を扱う企業や大学から同様のコンセプトの特許が出願されています。[7]

4 H. Takenaka, et al., Nature Photonics **11**, 501 (2017)
5 S. –K. Liao, et al., Nature **549**, 43 (2017)
6 H. Endo, et al., Optics Express **26**, 23305 (2018), H. Endo, et al., OSA Continuum **3**, 2525 (2020)
7 M. Legre and B. Huttner, EP 3337063 A1 (2016), E. J. A. Ling, et al., WO 2019/139544 A1 (2019)

04 第4章 要素技術と要求条件

【必要となるであろう要求条件】

物理レイヤ暗号を衛星 – 地上局間通信に適用するには、衛星 QKD 技術と同様の、プロトコル開発、捕捉追尾系のようなリンク確立のための技術開発、高速・高感度な検出器技術開発が必要となります。一方、モバイル通信への適用には、高周波帯 (ミリ波、テラヘルツ波、LED) に適したプロトコル開発が必要です。

③衛星－地上ネットワーク連携技術（適応的経路選択技術）

【どんな技術か】

安全性の要求レベルなどのユーザ要件や天候などの自然条件を考慮して、衛星と地上を合わせたネットワーク全体としての最適な経路や伝送プロトコル (QKD ／物理レイヤ暗号など) を選択し、秘匿通信のサービスを途切れることなく提供するための技術です。（衛星 QKD による安全な基幹ネットワーク（P12）を参照）

【何に／何故必要か】

例えば、衛星 QKD ／物理レイヤ暗号は曇天では実施できないため、晴れている地域の地上局を選択する必要があります。致命的な遅延なく秘匿サービスを提供するためには、この地上局の選択に応じて地上ネットワーク側の経路も適切に変更する必要があります。

【国内外現状】

衛星光通信における天候に基づいた地上局の変更はサイトダイバーシチと呼ばれ、NICT ではこれまで研究開発を重ねてきています。[8]

【必要となるであろう要求条件】

気象情報などの通信路に関する情報を収集し、衛星ノードや地上ノードなどで共有するための技術が必要になります。また、地上の様々な場所で衛星とのリンクの確立するために、地上局の小型化、可搬化、及び船舶等への搭載を可能にする技術が求められます。

（3）量子ネットワーク

①量子インターフェース

【どんな技術か】

異なる種類の量子物理系の間で量子情報を変えずに伝送する技術です。量子メディア変換とも呼ばれています。

【何に／何故必要か】

空間的に離れたノードを構成する物質量子系の光子を介した量子接続を実現するために必要とされています。

【国内外現状】

物質量子系から蛍光光子を発生させ通信波長帯光子へ変換した実験が報告されています。[9,10]また、光子を介して空間的に離れた 2 つの物質量子系の量子接続を形成した例が報告されています。[11]

8 K .Suzuki, et al., ICSO2014, または OBSOC
9 T. Walker, et al., Physical Revew Letter **120**, 203601 (2018).
10 M. Bock, et al., Nature Communications **9**, 1998 (2018), V. Krutyanskiy, et al., npj Quantum Information **5**, 72 (2019)
11 B. Hensen, et al., Nature **526**, 682 (2015), W. Rosenfeld, et al., Physical Review Letter **119**, 010402 (2017), Y. Yu, et al., Nature **578**, 240 (2020)

04 第4章 要素技術と要求条件

【必要となるであろう要求条件】

送信元の物質量子系と光子の間に量子相関を生成する量子もつれ操作技術が必要となります。送信元と送信先で発生した 2 つの光子の干渉を高効率で測定する・高性能光子検出器が必要です。光子が伝搬して干渉測定を行い、その後に物質量子系への操作を行うまで量子状態を保持しておくための量子メモリが必要となります。

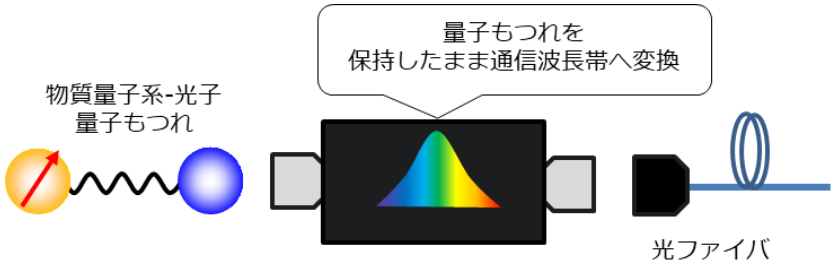


図 21　量子インターフェースの役割

②量子中継

【どんな技術か】

中継点に量子接続したノードを複数配置することにより長距離の量子情報伝送を可能とする技術です。

【何に／何故必要か】

量子状態は複製することが原理的に不可能ですので、通信路の損失による信号の減衰を増幅で回復することはできません。そのため量子接続の長距離化には量子中継が必要となります。QKD の長距離化にも適用可能です。

【国内外現状】

国内外で量子もつれ交換、量子もつれ純化、量子メモリを用いる標準的手法での研究開発が進められており、量子メモリの性能向上が実現のカギとされています。[12] また、国内では量子メモリを使用しない全光量子中継方式が提案されており、[13] 実証実験が行われています。[14]

【必要となるであろう要求条件】

標準的手法では送信元と送信先、および中継点に配置されたノードで、物質量子系と光子に量子相関を生成し、量子もつれ交換、量子もつれ純化などの量子もつれ制御技術に加えて、一連の操作が終了するまで量子状態を保持する量子メモリが必要です。全光量子中継方式では量子メモリが不要となります。量子もつれ操作で光子の干渉を高効率で観測するための高性能光子検出器が必要となります。

12　S. J. Yang, et al., Nature Photonics **10**, 381(2016)
13　K. Azuma, et al., Nature Communications **6**, 6787 (2015)
14　Y. Hasegawa, et al., Nature Communications **10**, 378 (2019), Z.-D. Li, et al., Nature Photonics **13,** 644 (2019)

04 第4章 要素技術と要求条件

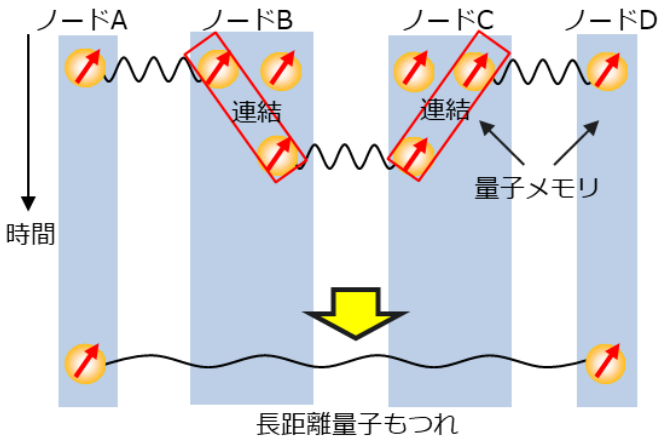


図 22　量子中継の仕組み

③多種量子ネットワーク制御管理

【どんな技術か】

QKD ネットワーク及び量子中継ネットワークを含む様々な将来アプリケーションの要件／要求を満たす多種類の仮想量子ネットワーク（量子コンピュータの仮想化を含む）を、同一物理ネットワーク網で安定的かつ安価に提供可能とする技術です。

【何に／何故必要か】

ネットワーク事業者が管理する物理機器を節約して低コスト化を図りつつ、多様なアプリケーション要件／要求（QKD における暗号鍵サイズや、通信性能、量子アプリケーションの安定性等）を満たすことが必要です。

【国内外現状】

国際標準化機関では、ITU-T SG13 おいて QKD ネットワークを対象とした SDN（Software Defined Network）制御及び仮想化について議論中です。[15] 一方、IRTF において量子インターネット（量子中継ネットワーク）について議論中です。[16] さらに、欧米では、量子ネットワークに関するプロジェクトが既に開始されています。例えば、米国では、大統領府の米国量子調整局が量子情報科学の国家戦略の報告書 [17] を公開しており、欧州では、オランダのデルフト工科大学が、量子インターネットを含む将来の量子ネットワークに関する報告書 [18] を公開しています。

【必要となるであろう要求条件】

様々なアプリケーションの要件／要求を満たす仮想量子ネットワークを構築し、さらにネットワークのトラヒック変動や障害検知などの状況変化に対応するため、経路選択や経路切り替え、リソース割当などを高速かつ効率的に行う仕組みが、アプリケーションの安定性向上の点で重要です。

また、古典ネットワークにおいて盛んに研究開発されているポリシー制御（例えば SDN）やネットワーク内処理技術（例えば情報指向型通信やネットワークコーディング）などを応用することが有効と考えられます。

さらに、制御管理機構の安全・安心を保証するための高度セキュリティ技術や、グローバルな仮想量子ネットワークを実現するための地上系・衛星系統合技術も将来的に求められます。

15　ITU-T SG13 Y.QKDN-SDNC (June 2020)
16　ITRF QIRG-ID: “Applications and Use Cases for the Quantum Internet”(draft-irtf-qirg-quantum-internet-use-cases-04) (January 2021)
17　“Quantum Frontiers: Report on Community Input to the Nation’s Strategy for Quantum Information Science, “ The White House National Quantum Coordination Office (October 2020)
18　“Creating the Quantum Future – QuTech Annual Report 2019,” Delft Univ. of Tech. (March 2019)

04 第4章 要素技術と要求条件

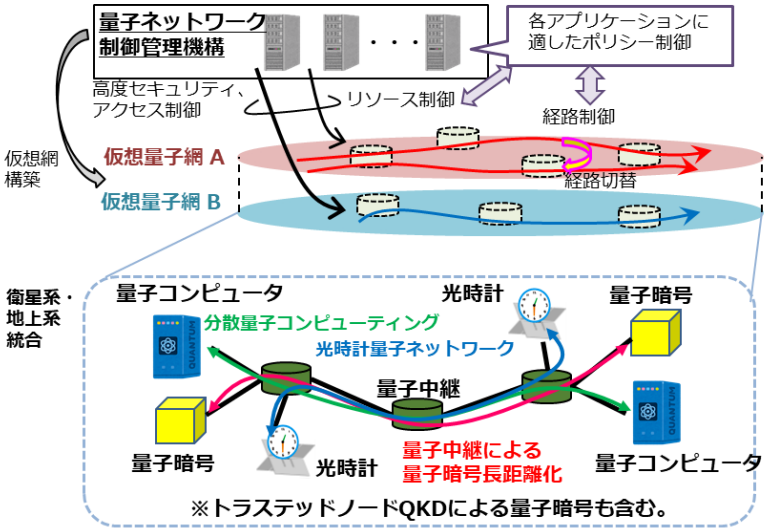


図 23　量子ネットワークの仕組み

④量子センサネットワーク（光時計量子ネットワーク）

【どんな技術か】

量子効果を利用して物理量を計測するデバイスは量子センサと呼ばれています。光周波数帯を用いる原子時計は光時計と呼ばれますが、重力を計測する量子センサとしても用いられます。光時計を光ファイバや自由空間で接続するコヒーレントリンクでは、量子接続技術を適用しなくても時空間情報配信や重力クラウドセンシングが可能となります。量子接続に拡張した光時計量子ネットワークでは、物理法則が許す限界まで計測速度が短縮されます。

【何に／何故必要か】

時空間情報として次世代通信の高精度タイミング配信、コヒーレント光通信の位相同期、超長基線干渉計などの実現に必要とされます。重力センサとして地中の空洞、マグマだまり、海底変動等の監視に有効と考えられています。

【国内外現状】

全欧州で光時計を繋ぐ全長 2,000km 以上のコヒーレントリンクを構築中です。[19]国内でも理研、東大、NICT などによりコヒーレントリンクの研究開発が進められており、全長 240km のリンクが報告されています。[20] 光時計量子ネットワークは提案のみで実現例はまだ報告されていません。[21]

【必要となるであろう要求条件】

光時計の持つ周波数精度を忠実に伝送するコヒーレントリンクが必要です。量子接続を付加するために、光時計を構成する原子やイオンの量子状態を光子経由で接続するための原子やイオンと光子の量子インターフェースが必要となります。光時計間のファイバ長が 100km を超える際には量子中継が必要となります。

19　https://www.clonets.eu/clonets-consortium.html
20　T. Akatsuka, et al., Optics Express **28**, 9186 (2020)
21　P. Komar, et al., Nature Physics **10**, 582 (2014)

04 第4章 要素技術と要求条件

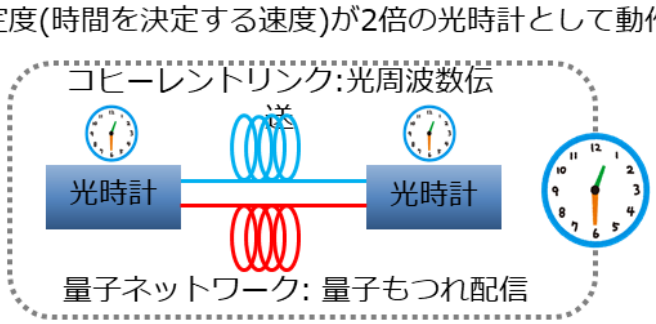


図 24　光時計量子ネットワーク

⑤量子コンピューティング（イオントラップ量子コンピュータ）

【どんな技術か】

イオントラップ中でレーザー冷却された原子イオンを量子ビットとし、トラップ電場による振動運動のフォノンを量子バスとして全量子ビットが結合されたイオントラップ量子コンピュータを形成できます。イオンと光の量子インターフェースを付加したイオントラップ量子コンピュータは光接続イオントラップ量子コンピュータと呼ばれます。

【何に／何故必要か】

単体のイオントラップ量子コンピュータでは、原理的および技術的制約により 50 量子ビット程度が大規模化の限界と考えられています。複数のイオントラップ量子コンピュータを全量子的に光接続することで大規模量子計算が可能になると考えられています。

【国内外現状】

光接続機能を有しないイオントラップ量子コンピュータとしては 32 量子ビットまでの実機が米国、ヨーロッパで実現し、クラウド量子計算サービス提供を開始[22]しています。光接続機能を有するイオントラップ量子コンピュータは実現しておらず、米国、ヨーロッパで 50 量子ビットを目標として研究開発が進められています。[23]国内ではムーンショット型研究開発事業での研究開発が開始しています。[24]

【必要となるであろう要求条件】

単体のイオントラップで量子計算が可能な 10 量子ビット程度での量子計算が実行可能で、光子との量子インターフェースを持つ高機能イオントラップが必要です。イオントラップで生成された光子の波長を光スイッチに接続するために光通信波長帯に変換する量子波長変換技術が必要となります。光接続操作を行うために 2 光子干渉観測技術、高性能光子検出器が必要です。

22　https://ionq.com/, https://www.aqt.eu/
23　https://www.aqtion.eu/
24　https://www.jst.go.jp/moonshot/program/goal6/index.html

04 第4章 要素技術と要求条件

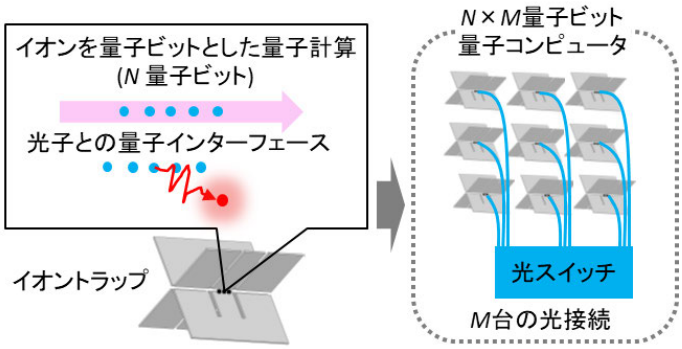


図 25　光接続イオントラップ量子コンピュータ

⑥量子コンピューティング（超伝導量子コンピュータ）

【どんな技術か】

極低温に冷却された超伝導電気回路は量子力学的に振舞うことから、超伝導量子回路と呼ばれています。超伝導量子回路は設計自由度が高く、量子ビット、共振回路、導波路、結合回路等の作りこみが可能です。これら回路要素から構成される、量子ビットゲート操作・状態測定が可能な多数の量子ビットから成る系を超伝導量子コンピュータと呼びます。

【何に／何故必要か】

量子コンピュータは量子力学を計算過程に用いることで、特定の問題においては現在のコンピュータと比べて圧倒的な処理能力を持つとされています。高い設計自由度・集積可能性をもつことから、超伝導量子コンピュータは量子コンピュータの最有力候補の一つとして考えられています。

【国内外現状】

2019 年、Google は 53 量子ビットを含むサンプルにおいて量子超越性を実証しました。[25] このように、NISQ（Noisy Intermediate-Scale Quantum computer）[26] と呼ばれるエラー訂正を行わない数 10 量子ビットからなる超伝導量子コンピュータの研究開発が盛んにおこなわれています。国内では、光・量子飛躍フラッグシップ・プログラム Q-LEAP、[27] ムーンショット型研究開発事業 [28] での研究開発が行われています。

【必要となるであろう要求条件】

コヒーレンス時間の長い量子ビットの研究開発が必要です。また、高速・高精度な量子ビットゲート操作、量子ビット測定、量子フィードバックに必須の低反射・ロスのマイクロ波伝送技術、高精度なマイクロ波パルス生成技術、高感度なマイクロ波測定技術、高速信号処理技術も必要です。さらに、希釈冷凍機の冷却パワー増大、超伝導量子回路作製技術の再現性向上も必要です。

25　F. Arute, et al., Nature **574**, 505 (2019)
26　J. Preskill, Quantum **2**, 79 (2018) https://doi.org/10.22331/q-2018-08-06-79
27　https://www.jst.go.jp/stpp/q-leap/
28　https://www.jst.go.jp/moonshot/program/goal6/index.html

04 第4章
要素技術と要求条件

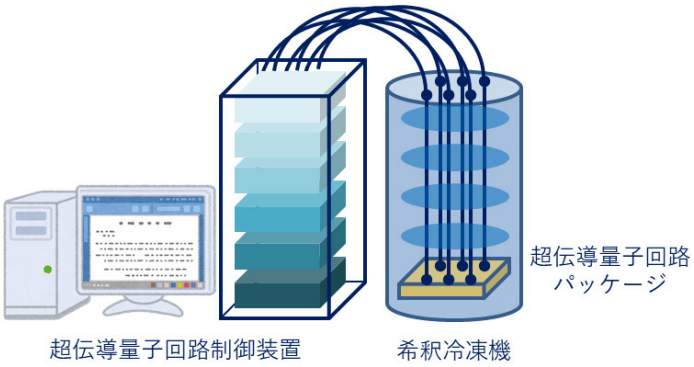


図 26　超伝導量子コンピュータ

05 第5章 研究開発ロードマップ

第 4 章の要素技術について、2020 年～ 2035 年頃を見据えたロードマップをまとめました。地上系及び衛星系の QKD ネットワークの研究開発ロードマップは次の通りです。

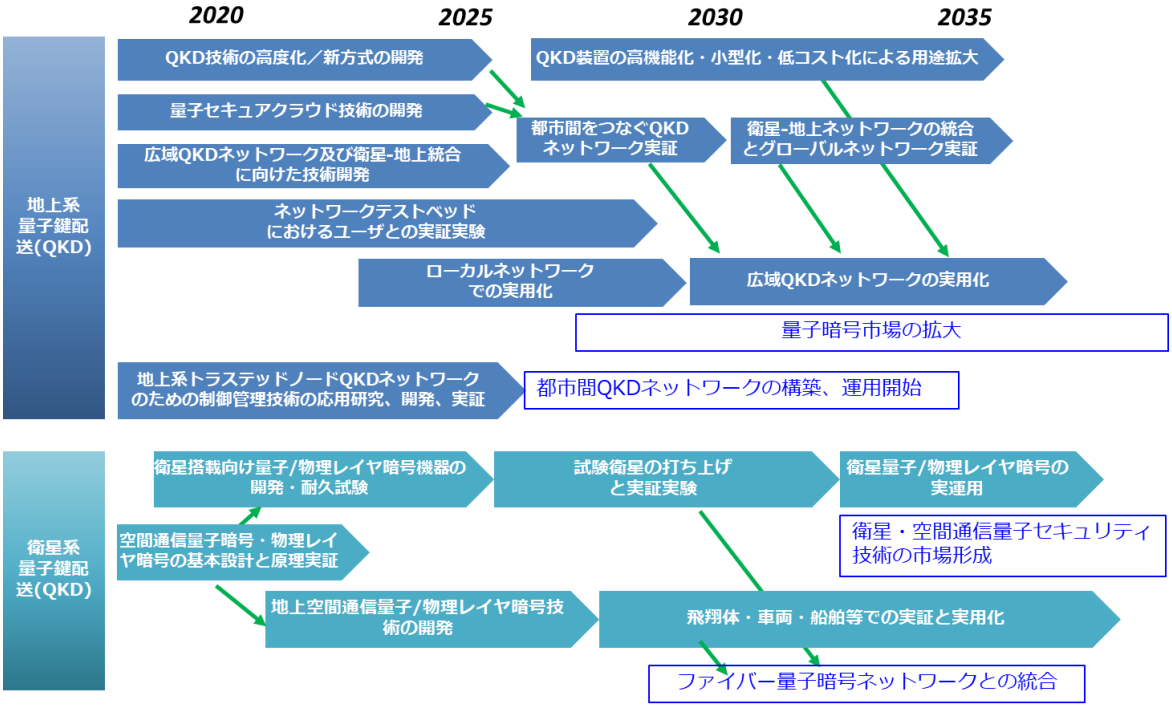


図 27　地上系・衛星系 QKD の研究開発ロードマップ

量子ネットワークの研究開発ロードマップは次の通りです。

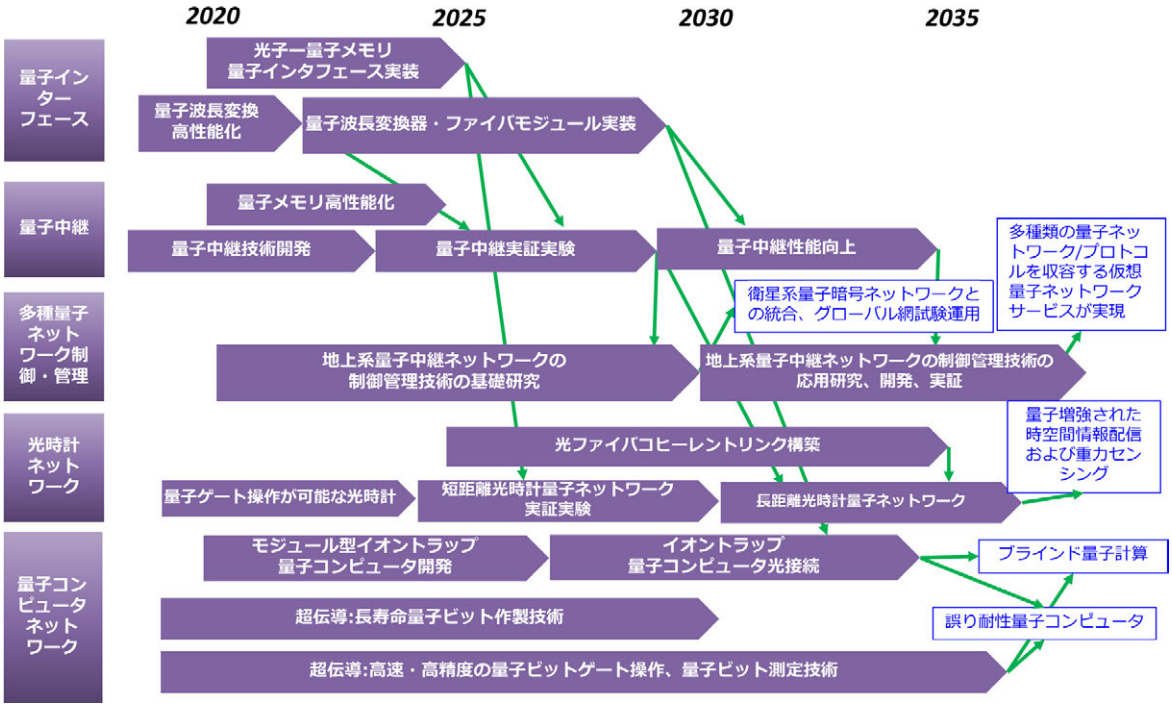


図 28　量子ネットワークの実現に向けた研究開発ロードマップ

06 第6章 推進戦略

1．全体像

今後、NICT が外部ステークホルダーと連携し、QKD ネットワークや量子ネットワークを社会に展開していく上で必要となる推進戦略を取りまとめました。

量子ネットワークの社会への展開を目指して、5 つの取り組み（（1）研究開発、（2）社会実装、（3）国内連携・国際連携、（4）制度設計、（5）人材育成）を一体的に進めることが必要です。

①研究開発	●継続的な研究開発の推進 ●研究成果の技術移転の推進 ●国家プロジェクトによる研究開発の推進
②社会実装	●テストベッドの構築 ●アプリケーション開発基盤の提供（ビジネスエコシステム確立） ●産業育成
③国内連携・国際連携	●大学・研究機関との連携 ●研究コミュニティの形成 ●コンソーシアム形成・支援 ●グローバルなパートナーづくり ●外国機関との連携プログラムの立ち上げ
④制度設計	●国際標準化の推進 ●評価・検定・認定制度の整備 ●サイバー保険への適用
⑤人材育成	●量子ネイティブの育成・確保 ●多様な量子人材の育成・確保 ●量子セキュリティ拠点の活用

図 29　量子ネットワークの社会への展開に向けた推進戦略（全体像）

2．個別推進戦略

（1）研究開発

● NICT における継続的な研究開発の推進

NICT は、国の計画・戦略や NICT 第 5 期中長期目標・計画に基づき、量子ネットワーク技術の研究開発や関連特許の確保に取り組みます。成果が出るまでに 5 ～ 10 年程度を要する分野については、継続的な投資を得られるよう研究の意義や成果のアピールをしつつ取り組みます。

● NICT における研究成果の技術移転の推進

NICT は、政府等と連携して、企業が技術をキャッチアップするための研究開発を推進することが必要です。また、NICT での基礎研究成果の技術移転がより円滑に行われるような制度の運用・改善が必要です。

●国家プロジェクトによる研究開発の推進

欧米などを中心に研究開発が進められている量子ネットワーク技術など、市場規模が不明確で企業の参加が難しい技術分野については、国家プロジェクト等により産学官の連携体制を構築し、研究開発を推進することが必要です。

06 第6章 推進戦略

（2）社会実装

●テストベッドの構築

NICT は、政府、企業等と連携し、量子技術イノベーション拠点を繋ぐオープンテストベッドを構築します。（量子技術プラットフォームの構築に向けた取組案（P37）を参照）

府省による国プロの成果を糾合して、日本のリソースの集約・有効活用を図るとともに、産学官の共同利用の仕組みを構築します。

●アプリケーション開発基盤の提供（ビジネスエコシステム確立）

NICT は、政府、企業、量子 ICT フォーラム等とも連携し、多様なレイヤにおける新しいサービス・ユースケースの検討・実証機会の提供、アプリケーションの開発強化、ビジネスエコシステムのモデル検討などを進めます。

●産業育成

NICT は、通信事業者・サービスプロバイダ等の量子ネットワーク分野への研究開発・社会実装の取り組みを推進し、量子ネットワークの普及・展開を加速します。

国内で量子ネットワークの主要な機器・部品の製造ができるよう、NICT は、国内のベンダー・部品メーカ等関連企業とも積極的に連携を行い、部品製造やビジネスモデルの創出を支援し、サプライチェーンの構築を推進します。NICT 発のスタートアップ企業の創出も視野に入れます。

（3）国内連携・国際連携

●大学・研究機関との連携

イオントラップ、超伝導など様々な方式の量子技術の研究開発が進められており、これらに対応できるよう、NICT は、他の研究機関と連携を進めるとともに、成果の量子通信以外での応用も視野に入れます。

量子ネットワークの実現に向けて、NICT は、量子中継技術、ネットワークアーキテクチャ、ソフトウェア等の研究開発強化のため、研究体制・他の大学・研究機関との連携を進めます。

●研究コミュニティーの形成

NICT は、ムーンショット研究開発制度、Q-LEAP 等の国家プロジェクトへの参画などにより、研究資金の獲得を進めるとともに、国家プロジェクトの参加者や大学・研究機関における研究者等が参画する研究コミュニティーの形成を推進します。

●コンソーシアム形成・支援

NICT は、量子 ICT フォーラム等を通じて企業・大学等の連携を推進します。

量子技術、インターネット研究者からなる産学官をメンバーとした量子ネットワークを推進するコンソーシアムが形成されおり、NICT は、このような学際的コミュニティーへの参画、支援を進めます。

●グローバルなパートナーづくり

NICT は、量子技術が国際競争や安全保障などにも関りが深いことを考慮しつつ、量子ネットワークの研究開発を加速するとともに国際的なテストベッドの構築に向け、グローバルな戦略的パートナー、標準化を行う上でのサポーターづくりなどを積極的に進めます。

06 第6章 推進戦略

●外国機関との連携プログラムの立ち上げ

NICT は、EU や NSF との連携枠組みなどを活用しながら、今後の研究開発や国際連携の方向性について議論を進めます。量子技術に関する研究開発の人的・財政的リソースが限られているなかで、日本の技術を世界で使えるようにしていくことに努めます。

（4）制度設計

●国際標準化の推進

NICT は、政府や企業等と連携し、量子ネットワーク技術（特に QKD ネットワーク技術）のグローバルな普及に向けて、国際電気通信連合電気通信標準化部門（ITU-T）や国際標準化機構・国際電気標準会議第 1 合同技術委員会（ISO ／ IEC JTC1）において国際標準化や戦略的な国際特許の出願を推進します。

●評価・検定・認定制度の整備

NICT は、政府、企業、量子 ICT フォーラム等と連携し、QKD 装置の適切な安全性評価手法の開発と、上記の ISO ／ IEC 等で開発される国際規格に準拠した形でのセキュリティ要件の文書化（いわゆるプロテクションプロファイル（PP）の作成）や、PP の運用体制の整備を推進します。

●サイバー保険への適用

NICT は、企業等と連携し、QKD 導入に対する保険適用や保険料額の減免について検討します。

（5）人材育成

●量子ネイティブの育成・確保

NICT は、政府、大学、企業等と連携し、量子人材育成プログラム NQC（NICT Quantum Camp）を通じた量子ネイティブを育成します。また、量子アルゴリズム、プログラミング高級言語、アーキテクチャなどフルスタックで考える人材、全体をデザインできる人材を育成についても検討します。

NICT は、NICT における学生・社会人インターンの受入れ、大学との連携体制の拡充、魅力的なキャリアパスの整備などにより研究人材を継続的に確保します。

●多様な量子人材の育成・確保

NICT は、研究だけでなく、技術、知財管理、経理など、様々なスキルを持った人材を確保し、NICT の組織として強靭化を図ります。

●量子セキュリティ拠点の活用

NICT は、協創スペースを活用した人材育成、セミナーなどの実施、拠点を結ぶオープンテストベッドを活用した実践的な人材育成プログラムを進めます。

06 第6章 推進戦略

・量子技術イノベーション拠点を繋ぐネットワークインフラを順次整備
・府省による国プロの成果を糾合 ⇒ 日本のリソースの集約・有効活用
・産学官の共同利用の仕組みを構築（オープン/クローズ戦略）

第1段階（2022年頃）：関東圏（量子コンピュータ、量子暗号・中継、光格子時計）
第2段階（2025年頃）：都市間（仙台、東京、大阪など。量子技術の集約）
第3段階（2030年頃）：衛星・地上網の統合（日本全土）
第4段階（2035年頃）：グローバルネットワーク化

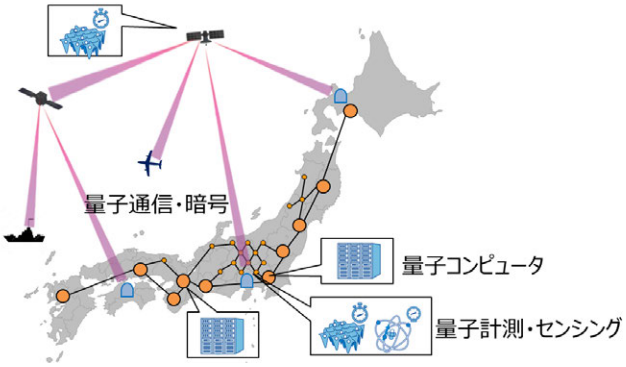


図 30　量子技術プラットフォームの構築に向けた取組案

07 第7章 おわりに

本ホワイトペーパーでは、量子ネットワークに関する社会像やユースケース、要素技術や 2021 年から 2035 年までの研究開発ロードマップ、推進戦略をまとめました。

量子ネットワークについては、国内外において QKD の社会実装に向けた取り組みや量子インターネットを見据えた研究開発が強力に推進されています。NICT は、今後、第 5 期中長期計画（2021 年度～2025 年度）に従い、本ホワイトペーパーの推進戦略を踏まえて、国内外における有識者、企業、大学、研究機関等と連携し、量子ネットワークの社会への展開に向けて取り組みを進めていきます。

また、今後の国内外の動向や研究開発の進展を踏まえて、本ホワイトペーパーのブラッシュアップを進めていきます。

参考

ホワイトペーパー作業メンバー一覧

朝枝 仁、泉 映絵、石谷 寧希、井出 真司、井戸 哲也、井原 章之、遠藤 寛之、大坪 望、菅野 敦史、斉藤 嘉彦、佐々木 明彦、佐々木 雅英、庄野 志保、関根 徳彦、仙場 浩一、武岡 正裕、達本 吉朗、寺井 弘高、豊嶋 守生、Nils Nemitz、蜂須 英和、早坂 和弘、古澤 健太郎、三木 茂人、宮澤 高也、松園 和久、諸橋 功、柳沢 光太郎、山口 祐也、吉原 文樹

国立研究開発法人
情報通信研究機構
National Institute of Information and Communications Technology

量子ネットワークホワイトペーパー

2021 年 3 月 31 日　初版発行
ISBN978-4-904020-11-1

国立研究開発法人情報通信研究機構

〒184-8795　東京都小金井市貫井北町 4-2-1

E-mail　nict-idi-wp@ml.nict.go.jp
URL　https://www2.nict.go.jp/idi/