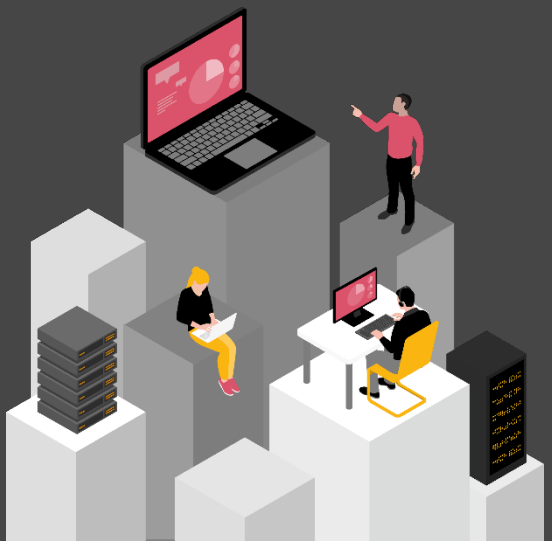
Emerging Technology Insights

Tech Translated: Quantum Cryptography
量子技術と暗号

2024 年 11 月



PwC コンサルティング合同会社
PwC Intelligence　マネージャー　柳川 素子
Technology Laboratory シニアマネージャー 北野 剛史

Tech Translated: Quantum Cryptography　翻訳版

s+b a PwC publication

量子暗号とは何か

サイバーセキュリティは、今日の企業が直面している最大の課題の一つだが、量子物理学を利用して問題解決を行う量子コンピュータの台頭により、既存のセキュリティシステムは前時代的なものになる恐れがある。現在の暗号化技術は、基本的には、非常に難しい数学の問題にすぎない。とはいえ正しいパスワードがない場合、現状で最も強力なコンピュータでさえ、その暗号を解読するために必要な何十億もの計算を行うには、数十年、場合によっては数百年かかると言われている。しかし大幅に向上した処理能力を持つ量子コンピュータが、この状況を一変させる可能性がある。PwC 英国法人のエマージングテクノロジーアドバイザリー シニアマネージャーである Kei Kumar は、「今日の初期段階の実験から、量子コンピュータが現時点で最高レベルの暗号を数時間、あるいは数分で解読できるようになるのは時間の問題であることがわかっている。そうなれば、オンラインコマースやコミュニケーションを成り立たせている現状のセキュリティフレームワークは完全に弱体化してしまう」と述べている。

量子コンピューティングは、ユーザー名とパスワードでアカウントにログインするといったインターネット上のあらゆる安全な通信を脅かす。現時点では解読不能な暗号技術に依拠した分散型アーキテクチャで構成されている、暗号通貨セクターに対する脅威にもなる。また、個人のクラウドドライブから病院のデータベースまで、あらゆる種類の保存された情報にも影響を及ぼす。

新興分野である量子暗号技術は、今日のデジタル情報がいかに脆弱であるかを明らかにするものだ。それと同時に、量子コンピュータによるハッキングに対抗するための技術の構築を目指している。

どのようなビジネス上の問題に対処できるか?

今日の初期段階の量子コンピュータでさえ、特定の種類の問題に関しては、最高性能のスーパーコンピューターよりも指数関数的に高速に結果を導くことが可能だ。これは、人類が複雑な課題を解決する能力に革命をもたらすと期待されるが、それと同時に、新たな課題を生み出す可能性もある。Kumar は、「これまで暗号化されたデータは、コンピュータの性能向上により古いアルゴリズムが解読可能になるまで、少なくとも平均 30 年間は安全だと想定されていた。しかし、量子コンピューティングが成熟すれば、そのバッファが完全になくなる可能性がある」と指摘する。

量子コンピューティングが暗号化に及ぼす脅威は、長らく理論上のものであったたが、2023 年にはそれが現実になったとの研究が報告された。

PwC のサイバーリスクに関する調査（Global Digital Trust Insights）2024 年版の結果では、サイバーセキュリティがすでにシニア IT リーダーたちの最大の懸念事項の 1 つとして挙げられている。量子コンピューティングの進化に伴い、将来的にサイバー脅威の中核になっていくはずだ。時代の流れに遅れることなく耐量子暗号が進化すれば、これらの脅威への対抗策になるだろう。

どのように価値を生み出すのか?

「量子コンピューティングによって何らかの影響を受けない業界はほとんどない」と PwC 米国法人の量子コンピューティング研究ディレクター、Arit Kumar Bishwas は説明する。「良いニュースは、量子研究者がこれらの脅威を研究する中で、脅威を軽減する優れた方法を見つけただけでなく、そのプロセスの中でセキュリティを保証するまったく新しい方法も発見していることだ」

量子暗号技術は 2007 年にジュネーブの地方選挙の公正性を確保するために初めて導入された。その後、通信や金融などの分野で試行が続けられ、新しい情報セキュリティの可能性を秘めつつ成熟を続けてきた。量子技術への民間投資は急増しており、2021 年と 2022 年には 20 億米ドルを超えるベンチャーキャピタルの資金が市場に投入された。また、業界と政府関係者の双方が「Y2Q[1]」へのカウントダウンが始まったことを認識しており、新しい耐量子暗号標準の提案・交渉はすでに始まっている。

「既存のデータセキュリティフレームワークからの移行と、耐量子暗号時代におけるまったく新しいテクノロジー・プラットフォーム・システム導入の複数の側面で混乱が生じるだろう」と Bishwas は指摘する。「Y2Q は、Y2K バグ[2]と同様の重大な脅威だが、より規模は大きくなる。そして Y2Q に必要な移行を円滑にナビゲートできる企業には、Y2K の際と同様のビジネス機会が訪れる可能性がある」

誰が注意を払うべきか?

サイバーセキュリティの責任者は、量子コンピューティングの最新動向に常に注目しておくべきだ。特に、金融サービス、銀行・証券領域、ヘルスケア、エネルギー・資源、公共事業、運輸・物流、通信などの業界では、CTO だけでなくサイバーセキュリティチームやネットワークアーキテクチャチームにとっても重要である。

耐量子暗号への移行に企業はどのように準備すればよいか?

リスクの潜在的規模を理解するために、人・プロセス・テクノロジーの 3 つの柱を考慮する必要がある。まずビジネスプロセスにおける暗号の利用状況とその潜在的な役割に関する一覧表を作成・管理することから始め、組織のセキュリティ強化につなげる。同時に、社内外のテクノロジーで使用されている技術標準とプロトコルを確認し、エコシステム全体を対象としてサードパーティが管理するものを含めて検討する必要がある。最後に、量子技術のブレークスルーはいつでも起こり得ることを念頭に、今すぐ人材のスキルアップに投資すべきである。IT システム管理やソフトウェア開発に携わる全ての人材が、暗号技術に対する量子の脅威を認識し、その対処における自分の役割を理解することが求められる。

日本版解説

■量子暗号通信／耐量子暗号に関する現状

前段で翻訳した PwC “***strategy+business* magazine**”の記事で解説されているように、量子コンピュータが従来の暗号技術を解読できるようになる恐れから、既存のセキュリティシステムを見直し、暗号技術を量子コンピューティング時代に合わせていく必要が生じている。量子コンピュータによる既存暗号の解読を防ぐ対応策としては、暗号の桁数を増やす、耐量子暗号（Post-Quantum Cryptography; PQC）[3]として新しい暗号方式に置き換える、量子鍵配送（Quantum Key Distribution; QKD：通信を送受信者する 2 者間で暗号鍵を安全に共有する方式）を使用する、既存の暗号方式と PQC を含む複数の暗号方式を組み合わせる、量子セキュリティ技術の開発を推進する、といった複数のパターンが考えられる。

特に大規模な企業システムや重要インフラ、セキュリティ要件の高い金融機関等の分野では、Y2K（2000 年問題）の際と類似した対応が必要になると考えられるが、Y2Q[1] のほうが事態は複雑である。2000 年という明確な期日のターゲットがあった Y2K と明確に異なるのは、量子コンピュータが現在の暗号を解読できるようになる Y2Q がどのタイミングになるかが不明で、対応のタイムラインに幅がある点だ。また、Y2K の場合は組織内部の既存のシステムの修正やアップデートに対応するという目的が明確だったが、Y2Q は外部からの不特定多数のアプローチに継続的に対処する必要が生じる。解決策についても、PQC、QKD をはじめ複数の手段があり、脅威に対する最適な対処方法が規定されているわけではない。Y2Q の正確な時期は不明だが、多くの専門家は今後数十年以内に到来すると予測する。国際組織クラウドセキュリティアライアンス(CSA)は 2030 年 4 月 14 日を「Y2K カウントダウン時計」の予想日としている [4]。

ビジネスの場面では、この脅威が既存システムや業務フローに与えるインパクトを考慮し、タイムラインを予測しながら具体的な対応策を検討・設計・実行することが求められる。広く対応が進められる中で発生が想定される主なビジネス機会について、プレイヤーごとに図表 1 にまとめた。関連プレイヤーは来るべき変化に備え、自社の立ち位置や役割を明確にしたうえで、自社内で必要な対応と社内外に向けたビジネス展開の双方を模索すべきだろう。

図表 1　量子暗号通信／耐量子暗号のビジネス機会（例）

プレイヤー種別	ビジネス機会
ハードウェアメーカー	対応製品（量子暗号通信の送受信機器、中継器等）開発・販売
ソフトウェアベンダー	対応ソフトウェア開発・販売・更新
セキュリティ関連ベンダー	新技術の実装支援、対応セキュリティ評価・コンサルティングサービス提供
通信事業者	対応通信ネットワーク構築・運用支援、量子鍵配信サービス提供（衛星通信等含む）
SIer	対応環境構築・移行/導入支援サービス
自動車製造業	自動運転普及時のセキュリティ対応
クラウドプロバイダー	対応クラウドサービス提供
研究機関・スタートアップ	関連技術や暗号アルゴリズムなどの研究開発

（出所）各種公開情報を基に作成

■各国の取り組み

量子暗号通信／耐量子暗号に関わる脅威にどのように備え、対応していくのかについて、現在世界的に検討が進んでいる。現在、各国が安全保障上のニーズも背景に技術開発を進めている段階にある。

図表 2 量子暗号通信／耐量子暗号に関する各国の取り組み

米国

- [PQC]米国立標準技術研究所（NIST: National Institute of Standards and Technology）が 2016 年から PQC の標準化計画を開始。米国土安全保障省(CISA:Cybersecurity and Infrastructure Security Agency）は 2022 年に、PQC への移行を推進するため「Post-Quantum Cryptography Initiative（PQC イニシアチブ）」[5]を設立。2024 年 8 月に大統領府が、NIST の新しい標準規格を発表 [6]
- [全体戦略]2018 年に国家量子イニシアチブ法が成立し、研究機関等の整備や投資を促進する方針が示された。2022 年の国防権限法（NDAA:National Defense Authorization Act）、CHIPS 法により内容の一部が改訂されている [7]

カナダ

- [PQC] PQC イニシアチブを立ち上げ、政府と研究者・企業が協力し、標準化を進めている
- [全体戦略] 2023 年 1 月に国家量子戦略（National Quantum Strategy）を制定 [8]し、量子技術の研究開発に 3 億 6000 万カナダドルを投資すると発表。Waterloo University の Institute for Quantum Computing(IQC)[9]をはじめ、最先端の研究を行っている機関がある

欧州（EU）

- [PQC]2024 年 4 月に EU が「PQC 移行のためのロードマップに関する勧告」[10]を発表。明確なマイルストーンとタイムラインを設定した計画策定を目指す
- [全体戦略]EU が 2030 年までに量子能力の最先端に立つことを目指し、Quantum Technologies Flagship Initiative を立ち上げ、財政支援を行っている [11]

オーストラリア

- [PQC]ACSC（Australian Cyber Security Center）が 2022 年 6 月に「Planning for Post-Quantum Cryptography」[12]を発表
- [全体戦略]2023 年 5 月に国家量子戦略（National Quantum Strategy）[13]を発表し、研究開発への注力を表明。2024 年 5 月に政府機関 Quantum Australia[14]を立ち上げ、産業とエコシステムの成長を支援する取り組みを行っている

中国

- [PQC]中国暗号研究協会（Center for Advanced China Research：CACR）が 2022 年に独自の PQC 標準化プロセスを開始し、2025 年ごろの商用移行を目指す [15]
- [全体戦略]量子暗号通信網の実用化で先行しており、国家戦略として 2025 年までに全国ネットワークの整備を目指している

韓国

- [PQC]2035 年までに国家の暗号システムを PQC に移行する計画を進めている
- [全体戦略] 2023 年 6 月に「大韓民国量子科学技術基本戦略」[16]を発表し、次世代暗号（量子耐性暗号）への転換計画を策定することを明記。

日本

- [PQC]総務省や NICT（情報通信研究機構）を中心に、研究開発が行われている。金融機関や電機メーカーが関与する形で、衛星を使った量子鍵配送の標準化に向けた検証実験なども実施されている
- [全体戦略] 2021 年 9 月「量子技術による新産業創出協議会（Q-STAR）」が発足し、政府は 2022 年 4 月に「量子未来社会ビジョン」、2023 年4月に「量子未来産業創出戦略」、2024 年 4 月に「量子産業の創出・発展に向けた推進方策」を策定。産学官連携の取り組みを進めている [17]

（出所）各種公開情報を基に作成

直近の取り組みの中で特に注目されるのは、米国立標準技術研究所（NIST）が 2024 年 8 月に発表した世界初となる標準規格である。連邦情報処理標準（Federal Information Processing Standards：FIPS）として 3 種類が最終決定された。世界初の PQC の標準規格として、量子技術における米国のリーダーシップを強調するとともに、政府機関や関連業界に対応を促している。PQC の標準規格化が今後各国・地域で進んでいくと考えられ、このような国家的な規格策定などの取り組みが日本でもどのように今後行われるのかなど、動向が注目される。

なお、各国の量子関連予算の投資額を見ると、現時点で最も規模が大きいのは中国である。公的な発表値はないものの、推定で約 150 億米ドルを超える国家予算が投下されている。韓国は、2035 年までに官民パートナーシップを通じて少なくとも 3 兆ウォン（約 23 億米ドル）を投資すると決定している [18]。一方で米国では国家科学技術会議（NSTC: National Science and Technology Council）が 2024 年に 9.68 億米ドルの量子関連研究開発費を見込んでいる [19]。比較すると米国の金額は小規模に見えるが、単年の予算であることに加え、民間企業の独自投資・研究開発や分野ごとに配分された予算、防衛関連予算など、この予算に含まれない金額があると想定され、実質としてはより大規模な額が投入されていると考えられる。日本（2024 年度予算）では、量子コンピュータ、ソフトウェア、セキュリティ、センシング等の各技術分野の取り組みとイノベーション創出のための基盤的取り組みに対し、約 368 億円が予算計上されている [20]。また、日本の企業・大学等による量子技術分野の研究費は 1,322 億円（2022 年度）で、AI やバイオテクノロジーよりは小規模なものの金額は拡大傾向にある [21]。日本における投資が技術振興やビジネス化につながるか、中国の多額の投資がどのような成果をもたらすか、他国の今後の戦略によって予算がどのように変化していくか、といった点を今後も注視する必要がある。

■「量子インターネット」まで広げた発想を

さらに量子技術関連の論点をネットワークの観点で拡大して考えた際には、「量子インターネット」の概念が注目される。これは遠隔地にある量子コンピュータ端末をつなげ、量子ビットの転送を可能とするネットワークを指す。具体的な方法としては、衛星・地上網、既存インフラ、プラットフォームを統合する形で量子センサや量子コンピュータが接続された、量子暗号通信も可能とするセキュアな分散型の量子ネットワークの構築が想定される。量子インターネットを基盤とした世界像はまだ検討段階にあり、全容が明確に見えている訳ではない。とはいえ単独のまったく新しい仕組みとして現れるものではなく、既存のネットワークをアップデートする形も含め、ユーザー企業やユースケースの発掘・拡大が起こると考えられる。量子コンピュータを伴ったインフラ刷新の機会においては、暗号関連の対応にとどまらず、広く量子インターネットの領域を含める形での検討が必要になり、関連プレイヤーのビジネスチャンスにつながる可能性がある。

すでに量子インターネット網の構築に向けた動きは起こっている。米国では 2020 年 7 月にエネルギー省(Department of Energy)が国家量子インターネット開発の推進計画（Blueprint）を発表 [22]。2018 年 12 月に成立した国家量子イニシアチブ法に基づき、10 年以内に米国内の量子インターネット網のプロトタイプを構築することを目標にしている。欧州では QIA（Quantum Internet Alliance）[23]という団体が設立され、量子インターネットネットワークのプロトタイプの構築を目指し、40 以上の学術機関や研究組織、企業などが参加している。日本では、産学官連携コンソーシアムとして「量子インターネットタスクフォース（QITF）[24]」が 2021 年に設立されており、分散型量子計算のインフラを考えるうえで重要な取り組みになっている。

量子インターネットのユースケースとしては、セキュアな通信、ブラインド量子計算（セキュリティを担保しつつ量子コンピュータを利用する方式）、分散型量子コンピュータ（小規模の量子プロセッサを接続して大規模化する方式）などが挙げられる。これらの実現においては通信の領域にとどまらず、量子ソフトウェアの研究開発なども含め、広く産業化のインパクトがあると考えられる。関連分野の研究開発に関しては、現状ではまだ中小規模の事例しかないが、今後の大規模開発を目指して研究・投資のチャンスがあることは確かだ。量子コンピュータが実用化されるタイミングには、インフラとして量子インターネットを整備しておかなければならないという観点で、そう遠くない未来における量子技術の民生化を見据え、関連プレイヤーにはビジネスチャンスを生かすための対応検討と実践が求められるだろう。

[1] （訳注）Y2Q（Years to Quantum）：量子コンピュータが従来の古典コンピュータでは達成できない計算能力を持ち、現在の暗号を解読できるようになるタイミング
[2] （訳注）Y2K バグ：西暦 2000 年にコンピュータの誤動作が起こる可能性があるとされた問題。西暦を下 2 桁で管理していたシステムが 1900 年と誤認する懸念があり、プログラムの修正をはじめ、不具合に備えた鉄道や航空機の運航停止等の対応も行われた。日本では「2000 年問題」とも呼ばれた。
[3] 量子コンピュータが実用化された後も安全性を保つことが可能な暗号方式
[4] Cloud Security Alliance Sets Countdown Clock to Quantum, CSA, 2022/3/9: https://cloudsecurityalliance.org/press-releases/2022/03/09/cloud-security-alliance-sets-countdown-clock-to-quantum
[5] CISA Announces Post-Quantum Cryptography Initiative,U.S. Department of Homeland Security, 2022/7/6: https://www.cisa.gov/news-events/news/cisa-announces-post-quantum-cryptography-initiative
[6] FACT SHEET: Biden-Harris Administration Continues Work to Secure a Post-Quantum Cryptography Future, The White House, 2024/8/13: https://www.whitehouse.gov/ostp/news-updates/2024/08/13/fact-sheet-biden-harris-administration-continues-work-to-secure-a-post-quantum-cryptography-future/
[7] About the National Quantum Initiative, NATIONAL QUANTUM INITIATIVE, 2024/10/8 アクセス: https://www.quantum.gov/about/
[8] Canada's National Quantum Strategy, Government of Canada, 2024/10/8 アクセス: https://ised-isde.canada.ca/site/national-quantum-strategy/en/canadas-national-quantum-strategy
[9] Institute for Quantum Computing, Waterloo University, 2024/10/8 アクセス: https://uwaterloo.ca/institute-for-quantum-computing/
[10] Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography, European Commission, 2024/4/11: https://digital-strategy.ec.europa.eu/en/library/recommendation-coordinated-implementation-roadmap-transition-post-quantum-cryptography
[11] Quantum: What is it and where does the EU stand? , European Parliament, 2024/10/4: https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2024)760413
[12] Planning for Post-Quantum Cryptography, Australian Government; Australian Signals Derectorate, Australian Cyber Security Center, 2024/10/8 アクセス: https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/governance/planning-post-quantum-cryptography
[13] National Quantum Strategy, Australian Government, 2023/5/3: https://www.industry.gov.au/publications/national-quantum-strategy
[14] Quantum Australia, 2024/10/8 アクセス: https://quantum-australia.com/quantum-australia
[15] 内閣府, "シンクタンク機能の試行事業の成果物", 個別調査分析 2　サイバーセキュリティ, 2023/3/14: https://www8.cao.go.jp/cstp/stmain/pdf/20230314thinktank/seikabutsu/shiryou3-1-02.pdf
[16] Korea Becoming the Global Hub for Quantum Economy, Ministry of Science and ICT, 2023/6/27: https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&bbsSeqNo=42&nttSeqNo=828
[17] 量子産業の創出・発展に 向けた推進方策, 内閣府, 2024/4/9: https://www8.cao.go.jp/cstp/ryoshigijutsu/240409_q_measures.pdf
[18] 2035 년까지 양자기술에 3 조 쏟는다…"선도국 기술수준 85% 달성", 2023/6/27: https://www.korea.kr/news/policyNewsView.do?newsId=148916914
[19] NATIONAL QUANTUM INITIATIVE SUPPLEMENT TO THE PRESIDENT'S FY 2024 BUDGET, 2023/12: https://www.quantum.gov/wp-content/uploads/2023/12/NQI-Annual-Report-FY2024.pdf
[20] "量子未来社会ビジョンの実現に向けた取組の推進", 内閣府 第 20 回　量子技術イノベーション会議 2024/7/26: https://www8.cao.go.jp/cstp/ryoshigijutsu/20kai/20kai.html
[21] 総務省統計局,「統計でみる 日本の科学技術研究 2023 年（令和5年）科学技術研究調査の結果から」, 2024/5: https://www.stat.go.jp/data/kagaku/kekka/pdf/05pamphlet.pdf
[22] U.S. Department of Energy Unveils Blueprint for the Quantum Internet at 'Launch to the Future: Quantum Internet' Event, U.S. Department of Energy, 2020/7/23: https://www.energy.gov/articles/us-department-energy-unveils-blueprint-quantum-internet-launch-future-quantum-internet
[23] Quantum Internet Alliance, 2024/10/8 アクセス: https://quantuminternetalliance.org/
[24] Quantum Internet Task Force, 2024/10/8 アクセス: https://qitf.org/

柳川 素子 | Motoko Yanagawa

マネージャー
PwC Intelligence

北野 剛史 | Tsuyoshi Kitano

シニアマネージャー
Technology Laboratory
Quantum Industry Laboratory

PwC コンサルティング合同会社

〒100-0004　東京都千代田区大手町 1-2-1 Otemachi One タワー　Tel：03-6257-0700