TOSHIBA

未来の量子社会経済を守るために今やるべきこと

はじめに

量子コンピューターに耐えうる経済の構築

近い将来のある時点での強力な量子コンピューターの登場が、今日私たちが慣れ親しんだコンピューティング環境を大きく変化させる可能性を秘めていることは明らかです。

主な影響のひとつは、サイバーセキュリティの多くの基本原則が損なわれ、市場に大きな懸念と不確実性がもたらされることです。量子コンピューターが実用的なデバイスとして存在する世界は、今日のデジタル経済を支えるセキュリティ基盤である**公開鍵暗号（Public Key Cryptography：PKC）**などの標準技術の安全性に疑問を投げかけるでしょう。

また、今日在るデータにも既に現実的なセキュリティ上の危険があります。サイバー攻撃者は、将来量子コンピューターを使い、将来でも高い価値のあるデータを解読できることを期待して、今からデータを収集する可能性があります。これは、「今収集して後で解読」（Harvest Now, Decrypt Later：HNDL）攻撃と呼ばれ、多くの専門家や政府関係者が警告している手法であり、今日サイバー攻撃者によってほぼ確実に行われています。量子コンピューター分野に多額の資金が投資され、開発が加速していることは、それを見越して将来のサイバー攻撃が今日計画されていることを意味しますが、問題は攻撃がいつどこで起こっているのか誰も検知できないことです。米国国土安全保障長官のアレハンドロ・マヨルカスは、2021年のRSAコンファレンスで次のように語っています。

> “現在すでに存在し、将来にわたって秘匿すべきデータの機密性を保護するために、今すぐ準備をしなければなりません。”

これらの理由から、量子産業界は現在および将来の脅威に対抗できるセキュリティ技術を開発することが不可欠です。現在、世界中で量子コンピューティング時代のセキュリティを再確立する為の技術がテスト・評価されており、その過渡期の始まりにいます。

これらの中で最も重要なものは、英国の商用ユーザーによってすでに試用されている量子セキュリティ技術である**量子鍵配送（Quantum Key Distribution：QKD）**です。

そのようなユーザー企業のひとつがEY（Ernst & Young）で、2022年にロンドンの**量子セキュアメトロネットワーク（Quantum-Secured Metro Network：QSMN）**の最初の顧客となりました。QSMNは、東芝のQKDハードウェアと量子鍵管理ソフトウェアを使用して、BTの光ファイバーネットワーク上に構築された最初の商用QKDネットワークです。EYはロンドンブリッジとカナリーワーフにあるふたつのオフィスをQSMNで結び、「今収集して後で解読」攻撃の可能性に対抗するQKDの能力を十分に検証することが出来ます。

量子コンピューティングが従来のサイバーセキュリティ手法にもたらす脅威は、経済的および技術的に広範囲にわたる影響を及ぼすため、組織はリスクを軽減するために今すぐ行動を起こす必要があります。ただし、量子セキュアネットワークの構築は、成熟するまでに数年かかる可能性があり、セキュリティの再検討と再構成を必要とする複雑な作業になります。QKDおよび新しい暗号標準である耐量子計算機暗号（Post-Quantum Cryptography：PQC）は、その中心となるでしょう。QSMNは、将来のセキュリティシステムを使用する必要性が大きく増す前に、その背後にある導入原動力を探るための完璧なテストベッドを提供します。

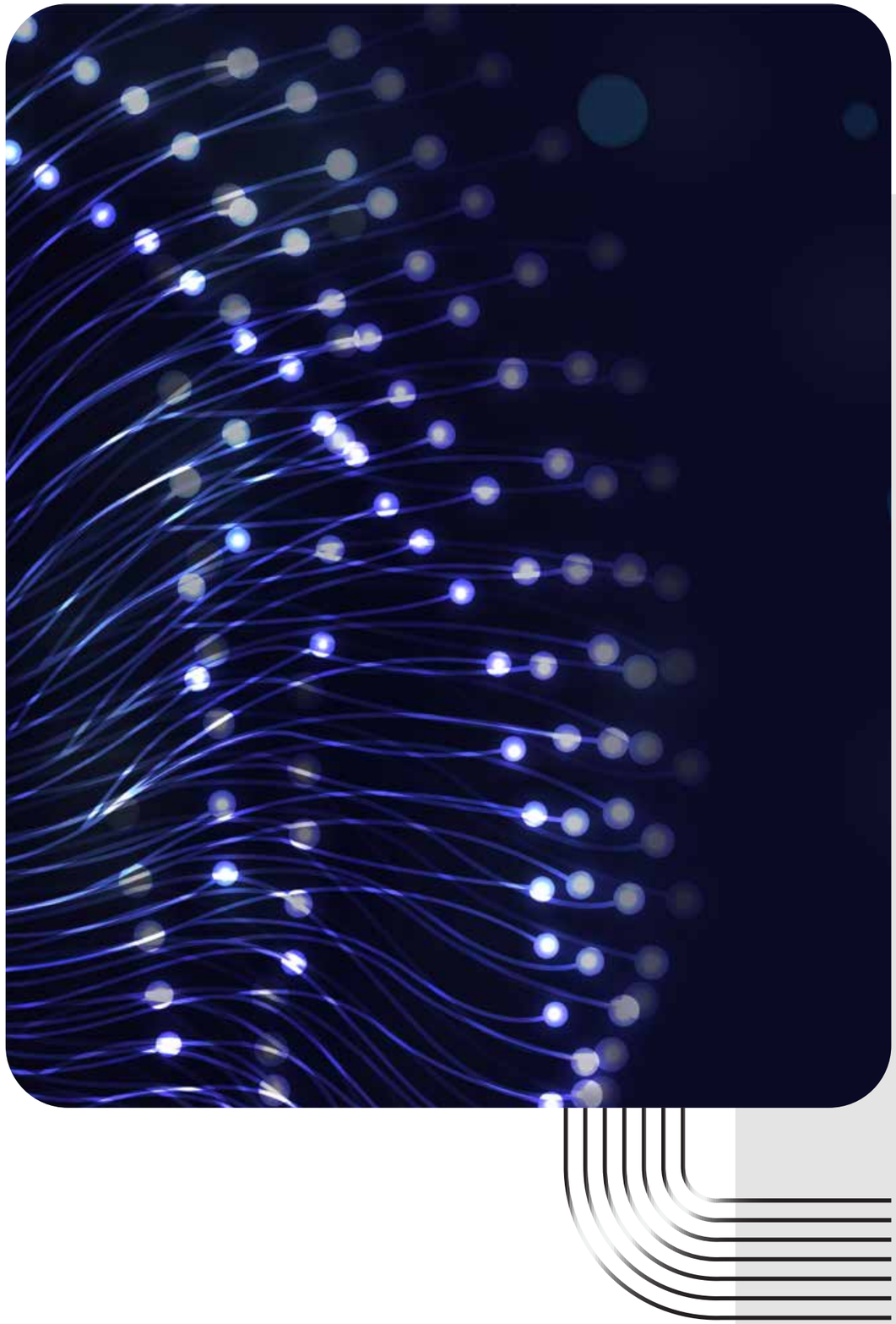
01

今日の世界における量子コンピューターの脅威

量子コンピューターが最初に提唱されて以来ずっと、専門家はそれが今日の暗号標準を脅かす可能性があることを懸念してきました。最も脆弱なのは、電子メール、HTTPSウェブ通信、暗号通貨といった多様なアプリケーションのセキュリティ基盤となっているRSAなどのアルゴリズムを用いて実装されたPKCです。

RSAや類似のアルゴリズムは、非常に大きな数の因数分解などある種の計算が現在の技術では非常に困難なことから、これまでのところうまくいっていました。理論的には、十分な時間をかければ古典的なコンピューターでもPKCを解読することは可能ですが、今日の最も強力なスーパーコンピューターをもってしても、現在の暗号システムで用いられている鍵長では、実際に解読にどれくらい時間がかかるかを考えればそれを破ることは非現実的です。

1990年代、数学者のピーター・ショアによって開発されたアルゴリズムは、量子コンピューターの基礎となる物理学が新しい数学を利用してこのタスクを従来のコンピューターよりも何桁倍も高速に実行できることを示した最初のアルゴリズムでした。その時点で、産業界は今日の暗号標準を量子コンピューターに耐性のある新世代のアルゴリズムとセキュリティ設計に置き換える必要があることに気づきました。



「今収集して後で解読」（HNDL）攻撃

専門家はすぐに2つ目の懸念を示しました。将来の量子コンピューターの存在は、現在保存されているデータのセキュリティも危険にさらすということです。これは、攻撃者が今日、大量の暗号化されたデータを収集し、量子コンピューターがその暗号鍵を解除できるようになるまで保存しておくことです。「今収集して後で解読」（または、「今盗み後で破壊」）と呼ばれる攻撃です。これは、財務情報や軍事機密などのデータの機密性が長い間損なわれないが故に、攻撃者にとって何年もの間有用であり続ける可能性があるという事実が悪用されたものです。

現時点での「今収集して後で解読」攻撃によってもたらされる脅威のレベルは、収集されたデータの種類によって異なります。ほとんどのウェブトラフィックでは、そのデータの価値が時限的か、価値そのものが低いため、リスクは低くなります。ただし、機密性の高い財務データや個人データについては、同じことが当てはまらず、数年または数十年にわたって機微情報であり続けます。

「今収集して後で解読」攻撃が実行されたかどうかを知ることは不可能ですが（そのような攻撃は他の形式のデータ傍受と区別できませんので）、その悪用は完全に論理的に可能です。金融機関や公的機関などの機密データなど、将来悪用可能なリソースとして利用できるデータを現在収集することは、悪意のある攻撃者にとって有益です。一方、PKCを弱体化させる能力を含む、高度なコンピューティングタスクを実行できる最初のデバイスを開発するために企業や国家が互いに競い合う中、量子コンピューティングへの投資は指数関数的に増加し続けています。

組織にとってのリスクは、量子コンピューターがPKCを破ることができる時点が近づいているということだけでなく、そのようなブレークスルーが実現しても、目に見えない利点を享受するためにそれが公にならない可能性があることです。これが起こったという未確認の可能性があるだけで、組織、株主、規制当局などが、おそらく安全な機密データがまだ本当に安全であるかどうかを調べるために奔走し、金融セクターを不安定にする可能性さえあります。この不確実性に対する重要な防御策は、このようなブレークスルーが実現するかなり前に、量子安全技術に投資することです。

02

量子安全への移行

量子リスクに対処するには、量子コンピューターに対抗できる
新しい暗号化アルゴリズムの開発から始まる、
ふたつの面での更なる進歩が必要です。
これは、米国国立標準技術研究所（NIST）の後援による
新しいPQCアルゴリズムの開発を通じてすでに起きています。

量子鍵配送（QKD）

量子安全な暗号化のセキュリティは、ふたつの要素に依存します。まず、暗号鍵の生成に使用されるアルゴリズムは、量子コンピューターによる解読に対して耐性があり、データ自体の復号が困難である必要があります。次に、暗号鍵はネットワーク全体に安全な方法で配送する必要があります。これには、安全でない公共ネットワークも含まれます。QKDは後者の例であり、今日では極めて安全に暗号鍵を配送するために使用できます。組織は次の点に注意する必要があります。

- QKDの安全性は、暗号鍵の各ビットがランダムな状態（または量子ビット）の一連の光子を使用して符号化される基本的な物理法則によって支えられています。これらの光子を傍受しようとすると、送信された正しいシーケンスが中断され盗聴が明らかになり、新しい暗号鍵が生成されます。
- QKDは、「今収集して後で解読」攻撃という問題に対する解決策となります。数学ではなく物理法則に基づいているため、量子コンピューターによる通信チャネルへの盗聴攻撃に対して将来にわたり耐性があることが証明されています。

量子セキュアメトロネットワーク（QSMN）

東芝が開発した技術とBTの光ファイバーインフラを基盤に量子セキュアサービスを実証するために設計された大都市圏規模のネットワークであるQSMNにより、顧客はQKDにアクセスすることができます。QSMNはロンドン市内とロンドン西部郊外に展開され、金融サービス分野などのBTの潜在顧客がいる大都市圏をカバーしています。

QSMNを要約すると以下のようになります。

- 顧客が量子セキュアテクノロジーの利用をテストし、セキュリティ戦略の一環としてテクノロジーを実装する方法を評価する仕組みを提供します。
- そのテクノロジーは、既存の光ファイバーネットワークに簡単に展開できます。また、PQCなどの将来の暗号化アルゴリズムと連携し、並行して評価する仕組みを提供します。
- そこで使われている東芝のQKDは、2014年からBTと共同で技術をテストするなど、20年以上の研究開発の結果である成熟した技術です。
- 潜在顧客がいる大都市圏で専用の高帯域エンドツーエンド暗号化リンクなど、量子技術で守られたさまざまなサービスを提供します。
- QKDは、セキュリティを保証することが必須な分野へ将来性のあるソリューションを提供するように設計されたハイエンド技術です（もちろん、マルウェア、ソフトウェアの脆弱性、または内部関係者の脅威などの個別のサイバーセキュリティの問題を軽減するわけではありません）。

03

量子セキュアメトロネットワークの運用：EYのケース

「未来はもうここにある。ただ広まっていないだけだ。」
EYの技術リスク担当役員である
ピアーズ・クリントン・タレスタッド氏は、
SF作家ウイリアム・ギブソンの言葉を引用しながら、
現実の世界に現在どのような量子技術が
存在するかについて述べています。

これはQKD導入の誘発であり、一方で、やがて復号できるようになることを期待して攻撃者が暗号化されたデータを今日ひそかに収集している可能性をも示しています。明日にもありえるデータ侵害が今日の世界で今まさに準備されているというのは、憂慮すべき予測です。

なぜ最大の課題のひとつが単純に「どこから手を付ければよいか」なのかを知ることは、顧客にとって多くの示唆に富んでいます。専門知識を習得するのは困難であり、既存の学習は多くの場合、ラボの実験結果または初期の試験結果に基づいたものです。EYのように実際にシステムを体験されたお客様からのフィードバックは非常に貴重です。

EYがQKDを導入した動機はふたつあります。まず、同社はM&Aビジネスコミュニケーションに関連する機密性の高い電話やビデオ通信を保護することが実行可能かテストしたいと考えていました。次に、金融企業の間でQKDセキュリティへの関心が高まっているため、EYは量子技術とビジネス変革で提供する幅広いコンサルティングの一環としてこの技術を提供できるか検討するために、この技術についてもっと学ぶ必要があると判断しました。

「私たちは、QKDをどのように使用できるかだけでなく、QKDをどのように将来の製品やサービスに統合したらクライアントに使ってもらえるかを学びたかったのです。」とクリントン・タレスタッド氏は述べています。

QKDとQSMNはセキュリティ分野ではまだ登場したばかりですが、英国の組織は学習段階に入り、金融業界内の多くの組織がEYにアドバイスを求めてくると、彼は確信しています。

> “私たちのクライアントも
> ユースケースを理解する必要があります。
> 私たちはすでに、複数のCIOとCTOが
> 全体的なセキュリティ体制と
> より広範な量子戦略の一部になり得る方法を
> 理解する為の支援をしています。
> 彼らは私たちが学んだことを
> 知りたがっています。”

現在、QSMNテストベッドではEYの内部イーサネットネットワークを繋ぐポイントツーポイントで光ファイバー接続されており、QKDと同様に、AES 256対称鍵（1分周期で更新）を使った従来の暗号装置が使用されています。EYは、実際のスループットと遅延に関する洞察を得るために、ネットワーク上でテストデータを送信しています。

クリントン・タレスタッド氏によると、EYのコンサルタント顧客が直面する最大の問題は、テクノロジーそのものよりも、リスク管理の観点からQKDのビジネスケースを理解することです。そのためには、まず組織が保護したい最も機密性の高いデータを特定する必要があります。過去にやったことがなければ気の遠くなるような作業ですが、多くのセキュリティアプローチの基本的な部分です。

「データとそのリスクとその寿命を理解する必要があります。それが完了すれば、QKDのビジネスケースが理にかなうところを突き止めることができます。」と彼は言います。このような演習を実施した組織はほとんどないため、これには時間がかかります。このプロセスに関するガイダンスを提供するアドバイザーを持つことは不可欠です。

QKDが対処するリスクはまだ先のように見えるかもしれませんが、「今収集して後で解読」攻撃の可能性があるため、組織は量子技術の進歩がもたらす影響について今すぐ計画を立て始めることが重要です。

> “EYは、クライアントが
> 今後数年間に考慮すべきことを含め、
> これをより広範な
> 量子戦略に組み込むのを支援します。”
> と彼は結んでいます。”

04

組織はどのように対応すべきか

現在の開発速度では、量子コンピューターが
データセキュリティを損なう時点は、おそらく10〜15年先のことです。
これは遠い先のリスクのように聞こえるかもしれませんが、
今すぐに対処すべきものなのです

QKDやPQCなどの量子安全技術への移行は、実装に何年もかかる複雑なプロセスになります。その技術は実際の条件下でテストする必要があり、組織はそれらを効果的に展開するために新しいスキルセットを備えたチームを構築する必要があります。このため、金融や政府など、最も影響を受けるセクターの組織は、長期的な課題になることを理解しながらも、できるだけ早くこの移行に取り組み始めることが重要です。

では、実際にどのように移行を達成していくか見ていきましょう。

データと暗号化の脆弱性を特定する

「今収集して後で解読」攻撃に対する組織の脆弱性は、保存するデータの時間的機密性と、そのデータを保護するために使用される暗号技術の強度の結果であり、さまざまなバリエーションがあります。このリスクを軽減するには、保存期間の長い重要なデータを識別して分類し、QKDやPQCなどの量子安全技術を採用するなどして、それに応じてこれらを保護する必要があります。

学習を始める

当然のことながら、量子の脅威に対する認識は依然として低いままです。つまり、データが危険にさらされている金融企業は、技術チームから経営陣まで広く意識を高める必要があります。同様に、量子安全技術を使用するために必要なスキルを見つけるのは容易ではありません。QSMNなどのネットワークは、実世界での学習に不可欠なプラットフォームを提供するだけでなく、金融機関が量子対応チームを構築するためのハブを提供します。

ロックインを回避する

他の新しい技術と同様に、顧客は後になって放棄またはアップグレードしなければならない設計に縛られることを心配しています。QSMNの主な強みのひとつは、QKDをサービスとして利用でき、特殊なインターフェースや大幅な変更を必要とせずに簡単に統合できることです。QKDは、標準のBT光ファイバー網で動作し、標準の2Uラックマウント装置としてお客様の建屋内に設置されます。また、暗号化されたイーサネットまたはIPリンクとして提供されるため、QKDによってバックアップされていても、実装は簡単です。これにより、組織は独自のネットワークを変更したり、高価な機器を購入して後でアップグレードしたりすることなく、その機能を評価できます。

結論

行動することが必要

幸いなことに、コンピューティングの歴史におけるほとんどの大きな変化とは異なり、
量子コンピューティングの出現は、そのメリットとリスクを事前に評価できる革命です。
歴史的に見て、パソコンやインターネットの登場など、コンピューティングにおける新しい機会は、
当初は過小評価される傾向があり、時間の浪費や誤った投資につながります。

対照的に、量子コンピューティングの時代は、予告された革命となるでしょう。これにより、組織は準備する時間を確保できます。このことから、金融などの主要セクターの組織は、来たるべき量子時代にできるだけ早く適応し始める必要があります。データセキュリティの観点からすると、最初の課題はリスクを理解することです。実はそれ自体が大変な作業です。あらゆる新興技術と同様に、量子システムを理解するためのスキルと知識を持つことはまだ本題ではありません。

本稿では、量子時代が急速に近づいていることが確実であることを検証しました。この新しい時代がどのように始まるかは誰にもわからないということは、依然として真実です。それが今日の暗号化プロトコルに疑問を投げかけるひとつのブレークスルーによってもたらされる可能性がある、と推測されることがよくあります。量子時代への移行は、一連の段階的な発見と発展によってもたらされる可能性もあります。

そのため、組織がいつどのように投資するかを評価することは非常に困難になります。2020年代初頭、企業はサイバー犯罪の増加から生じるリスクによる大きな課題に直面しています。確実な暗号化の道筋を失うことは、さらに悪いことです。QKDなどの先端の技術は今では特殊なものでも、常にそうであるとは限りません。ある時点で、QKD、PQC、およびその他の量子安全技術を日常のセキュリティの標準部分として統合する必要があります。組織が主導権を握り、このポスト量子の未来に今すぐ取り組むことが不可欠です。

BTについて

BTグループは、固定および移動体通信、および関連する安全なデジタル製品、ソリューション、サービスを提供する英国の大手プロバイダーです。また、マネージド通信、セキュリティ、ネットワークおよびITインフラストラクチャサービスを180ヶ国の顧客に提供しています。

BTグループは三つの顧客対応部門で構成されています。消費者部門は英国の個人および家族にサービスを提供します。BTビジネスは、英国および海外の企業と公共サービスをカバーしています。Openreachは、英国全土の650以上の通信プロバイダーである顧客に固定アクセスインフラストラクチャサービスを卸売りしている、独立して統治されている完全所有子会社です。

British Telecommunications plcはBT Group plcの完全子会社であり、BTグループの事実上すべての事業と資産を網羅しています。BT Group plcはロンドン証券取引所に上場しています。

詳細については、**www.bt.com/about**をご覧ください。

東芝について

東芝は、エネルギー・社会インフラから電子デバイスまで、幅広い事業でおよそ150年の経験を持つ知見と能力と、情報処理、デジタル、AI技術における世界最高水準の力を融合したグローバル企業グループです。これらの独自の強みは、誰もが享受できるインフラとつながるデータ社会の構築を支え、究極の目標であるカーボンニュートラルとサーキュラーエコノミーを実現する未来の実現を支えています。東芝は、東芝グループの基本理念である「人と、地球の、明日のために。」のもと、より良い世界につながるサービスとソリューションを通じて、社会の前向きな発展に貢献します。東芝グループは全世界に11万人の従業員を抱え、2022会計年度に年間3.4兆円（251億米ドル）の売上高を確保しました。

量子コンピューターによってもたらされるリスクから
データを守ることについて、詳しくはお問い合わせください。
quantum@toshiba.eu または **www.bt.com/media-enquiries**（英語）

東芝について詳しくは、こちらをご覧ください。
www.global.toshiba/ww/outline/corporate.html

このホワイトペーパーは、東芝欧州社が発行したWhite Paper「Securing the future quantum economy, today」を基に、
東芝デジタルソリューションズ株式会社によって日本語翻訳したものです。